

Model Services Agreement Combined Schedules

This agreement is issued by the Cabinet Office and is the copyright of the Crown. You may use and re-use the information within this agreement for commercial and non-commercial purposes without charge under the terms of the Open Government Licence v3.0, which is available at <http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/>. When you use any information within this agreement, you should include the following attribution, “Contains public sector information licensed under the Open Government Licence v3.0”, and include a link to the Open Government Licence.

For further information on Crown copyright policy and licensing arrangements, see [UK Government Licensing Framework - Re-using PSI (nationalarchives.gov.uk)](https://www.nationalarchives.gov.uk/information-management/re-using-public-sector-information/uk-government-licensing-framework/) or you can contact the Information Policy Team at [Public sector information enquiry - Contact us (nationalarchives.gov.uk)](https://www.nationalarchives.gov.uk/contact-us/public-sector-information-enquiry/)

No warranty is given by the Cabinet Office (or any other part of the Crown) as to the completeness of this document or its suitability for any purpose. This document is intended to be used only with legal advice and all users of this document do so at their own risk.

Amendments in this version

| **Version number** | **Date** | **Amendments** |
| --- | --- | --- |
| Version 1.02 | 5 June 2014 | Minor formatting changes and correcting paragraph numbering in Schedules 2.4 Annex 1 and 7.3 Annex 2. |
| Version 1.03 | 5 November 2015 | Schedule 2.2 definitions of Availability and Service Availability; Schedule 2.4 new definitions in Security Management Schedule; Schedule 8.3 model mediation agreement; Schedule 8.5 para 7.5 to allow normal recruitment; Schedule 9 Pensions Annexes additions in event Admission Agreement breached; various minor typing corrections; improved numbering and headings in Schedules. |
| Version 1.04 | 26 May 2016 | Schedule 8.3 minor amendments; Schedule 8.4 addition of Transparency Reports; other minor amendments. |
| Version 1.05 | 1 January 2018 | Introduction of Privacy Shield; minor corrections; improvements to clauses 16,17 and 19A and to Schedule 9; introduction of e-invoicing in Schedule 7 Part E; front cover amended to reflect open government licence terms. |
| Version 1.06 | 30 July 2018 | Update to Schedule 2.4 (*Security Management*), Staff Transfer 7.1 (*Staff Transfer*) including new Pensions Provisions for LGPS and NHS, Schedule 11 (*Processing Personal Data*). |
| Version 1.07 | 24 January 2019 | Update to Schedule 11 (*Processing Data*) – New annex on Joint Control. |
| Version 1.08 | 29 April 2019 | Update to Schedule 2.2 (*Performance Levels*), Schedule 2.4 (*Security Management*), Schedule 2.5 (*Insurance Requirements*), Schedule 5 (*Software*) - updated table only, Schedule 6.2 (*Testing Procedures*), Schedule 7 (*Charges and Invoicing*), Schedule 7.4 (*Financial Distress*), Schedule 7.5 (*Financial Reports and Audit Rights*) Schedule 8.4 (*Reports and Records Provisions*), Schedule 8.5 (*Exit Management*), Schedule 8.6 (*Service Continuity Plan and Corporate Resolution Planning*). |
| Version 1.08A | 4 June 2019 | Corrections to minor errors. |
| Version 1.09 | 10 July 2020 | New Transparency KPIs inserted to the KPI tables at Annex 1 to Schedule 2.2. New environmental requirements annexed to Schedule 2.3. New Assurance Process added to Security Management Schedule 2.4 at Part A to supplement Accreditation Process. New draft ethical wall agreement inserted at Annex 2 of Schedule 8.5. New TUPE staffing information tables inserted at Annex E2 of Schedule 9. Updating of pensions provisions to reflect the requirements at Part D at Schedule 9. |
| Version 1.09A | 12 November 2020 | New list of schedules inserted. New Standard Contract Clauses added to Schedule 11 at Annex 2 and Annex 3. |
| Version 2.0 | 11 April 2022 | Schedules renumbered. New Schedule 32 (*Intellectual Property Rights*) added. Updates to Schedules 1, 2, 3, 4, 5, 6 (Guidance only) 9, 12 (minor updates only) 18, 19 (minor updates only), 23 (very minor updates only) 24, 25, 26, 28, 29 (minor updates only), 30 (very minor updates only), and 31. |
| 2.1 | August 2023 | Addition of indemnities and move from breach of contract to indemnities for some liabilities to align model contracts. Updates to limitation of liability. Amendments to Power of Attorney provisions. Simplification of supply chain protection provisions. Updates to and simplification of the GDPR data protection clauses. Amendments to Modern Slavery clauses. Amendments to severance clauses. Updates to Security Management Schedule. Amendments to Insurance Schedule. Amendments to Software Schedule. Amendments to Charges and Invoicing Schedule. Amendments to Benchmarking Schedule. Updates to Change Control Procedure Schedule. Updates to Reports and Records Schedule. Amendments to Exit Management Schedule. Amendments to Staff Transfer Schedule. Amendments to IPR Schedule and updates to IPR provisions in Core Terms and Software Schedule. Numerous other minor changes and improvements. |
| 2.2 | February 2025 | Updates for the Procurement Act 2023, Security Schedules, and various other changes |
| 2.2A | September 2025 | Interim update – typos, errors, renumbering, alignment, Schedules 1, 5, 21, 27, 28 |

Model Agreement for Services

Schedules, Annexes and Parts

[Schedule 1: Definitions 9](#_Toc189823708)

[Schedule 2: Services Description 57](#_Toc189823709)

[Schedule 3: Performance Levels 60](#_Toc189823710)

[Part A: Performance Indicators and Service Credits 61](#_Toc189823711)

[Part B: Performance Monitoring 64](#_Toc189823712)

[Annex 1: Key Performance Indicators and Subsidiary Performance Indicators 68](#_Toc189823713)

[Part A: Key Performance Indicators and Subsidiary Performance Indicators Tables 68](#_Toc189823714)

[Part B: Definitions 79](#_Toc189823715)

[Schedule 4: Standards 84](#_Toc189823716)

[Annex 1: Sustainability 87](#_Toc189823717)

[Schedule 5: Security Management 94](#_Toc189823718)

[Part A: Authority-led Assurance 95](#_Toc189823719)

[Part B: Supplier-led Assurance 178](#_Toc189823720)

[Schedule 6: Insurance Requirements 259](#_Toc189823721)

[Annex 1: Required Insurances 262](#_Toc189823722)

[Part A: Insurance Claim Notification 262](#_Toc189823723)

[Part B: Third Party Public and Products Liability Insurance 263](#_Toc189823724)

[Part C: United Kingdom Compulsory Insurances 266](#_Toc189823725)

[Part D: Additional Insurances 267](#_Toc189823726)

[Schedule 7: Authority Responsibilities 269](#_Toc189823727)

[Schedule 8: Supplier Solution 272](#_Toc189823728)

[Schedule 9: Implementation Plan 274](#_Toc189823729)

[Annex A: Outline Implementation Plan 277](#_Toc189823730)

[Schedule 10: Testing Procedures 280](#_Toc189823731)

[Annex 1: Test Issues – Severity Levels 289](#_Toc189823732)

[Annex 2: Test Certificate 290](#_Toc189823733)

[Annex 3: Milestone Achievement Certificate 291](#_Toc189823734)

[Annex 4: Test Success Criteria 292](#_Toc189823735)

[Schedule 11: Charges and Invoicing 294](#_Toc189823736)

[Part A: Pricing 299](#_Toc189823737)

[Part B: Charging Mechanisms 303](#_Toc189823738)

[Part C: Adjustments To The Charges And Risk Register 306](#_Toc189823739)

[Part D: Excessive Supplier Profit Margin 312](#_Toc189823740)

[Part E: Invoicing and Payment Terms 313](#_Toc189823741)

[Annex 1: Pricing Mechanism 316](#_Toc189823742)

[Annex 2: Charging Mechanism and Adjustments 319](#_Toc189823743)

[Annex 3: Pro-forma Certificate of Costs 321](#_Toc189823744)

[Annex 4: Risk Register 322](#_Toc189823745)

[Annex 5: Allowable Assumptions 323](#_Toc189823746)

[Schedule 12: Payments on Termination 325](#_Toc189823747)

[Annex 1: Maximum Payments on Termination 332](#_Toc189823748)

[Schedule 13: Benchmarking 334](#_Toc189823749)

[Annex 1: Approved Benchmarkers 340](#_Toc189823750)

[Annex 2: Confidentiality Agreement 341](#_Toc189823751)

[Schedule 14: Financial Distress 348](#_Toc189823752)

[Annex 1: Rating Agencies and their Standard Rating System 358](#_Toc189823753)

[Annex 2: Credit Ratings and Credit Rating Thresholds 360](#_Toc189823754)

[Annex 3: Calculation Methodology for Financial Indicators 361](#_Toc189823755)

[Annex 4: Board Confirmation 366](#_Toc189823756)

[Schedule 15: Financial Reports and Audit Rights 368](#_Toc189823757)

[Part A: Financial Transparency Objectives and Open Book Data 371](#_Toc189823758)

[Part B: Financial Reports 373](#_Toc189823759)

[Part C: Audit Rights 376](#_Toc189823760)

[Schedule 16: Anticipated Savings 380](#_Toc189823761)

[Schedule 17: Governance 382](#_Toc189823762)

[Annex 1: Representation and Structure of Boards 387](#_Toc189823763)

[Schedule 18: Change Control Procedure 390](#_Toc189823764)

[Annex 1: Change Request Form 397](#_Toc189823765)

[Annex 2: Change Authorisation Note 398](#_Toc189823766)

[Schedule 19: Dispute Resolution Procedure 400](#_Toc189823767)

[Schedule 20: Reports and Records Provisions 409](#_Toc189823768)

[Annex 1: Records to be Kept by the Supplier 413](#_Toc189823769)

[Annex 2: Records to Upload to Virtual Library 414](#_Toc189823770)

[Schedule 21: Exit Management 425](#_Toc189823771)

[Annex 1: Scope of the Termination Services 437](#_Toc189823772)

[Annex 2: Draft Ethical Wall Agreement 441](#_Toc189823773)

[Schedule 22: Service Continuity Plan and Corporate Resolution Planning 452](#_Toc189823774)

[Part A: Service Continuity Plan 452](#_Toc189823775)

[Part B: Corporate Resolution Planning 461](#_Toc189823776)

[Annex 1: Exposure Information (Contracts List) 466](#_Toc189823777)

[Annex 2: Corporate Resolvability Assessment (Structural Review) 467](#_Toc189823778)

[Annex 3: Financial Information and Commentary 468](#_Toc189823779)

[Schedule 23: Conduct of Claims 470](#_Toc189823780)

[Schedule 24: Staff Transfer 473](#_Toc189823781)

[Part A: Transferring Authority Employees at Commencement of Services 477](#_Toc189823782)

[Part B: Transferring Former Supplier Employees at Commencement of Services 483](#_Toc189823783)

[Part C: No Transfer of Employees Expected at Commencement of Services 490](#_Toc189823784)

[Part D: Pensions 493](#_Toc189823785)

[Annex D1: CSPS 503](#_Toc189823786)

[Annex D2: NHSPS 505](#_Toc189823787)

[Annex D3: LGPS 510](#_Toc189823788)

[Annex D4: Other Schemes 516](#_Toc189823789)

[Part E: Employment Exit Provisions 517](#_Toc189823790)

[Annex E1: List of Notified Sub-contractors 525](#_Toc189823791)

[Annex E2: Staffing Information 526](#_Toc189823792)

[Schedule 25: Deed of Guarantee 536](#_Toc189823793)

[Schedule 26: Processing Personal Data 546](#_Toc189823794)

[Annex 1: Joint Controller Agreement 549](#_Toc189823795)

[Annex 2: International Data Transfer Agreement and International Data Transfer Agreement Addendum to the EU Commission Standard Contractual Clauses 557](#_Toc189823796)

[Part A: International Data Transfer Agreement 557](#_Toc189823797)

[Part B: International Data Transfer Agreement Addendum to the EU Commission Standard Contractual Clauses 585](#_Toc189823798)

[Annex 3: Standard Contractual Clauses for EU GDPR Compliant Transfers 592](#_Toc189823799)

[Part A: Processor to Controller Standard Contractual Clauses 592](#_Toc189823800)

[Part B: Controller to Processor Standard Contractual Clauses 605](#_Toc189823801)

[Part C: Processor to Processor Standard Contractual Clauses 625](#_Toc189823802)

[Schedule 27: Intellectual Property Rights 647](#_Toc189823803)

[Option 1 649](#_Toc189823804)

[Option 2 658](#_Toc189823805)

[Option 3 666](#_Toc189823806)

[Option 4 672](#_Toc189823807)

[Option 5 679](#_Toc189823808)

[Annex 1: Project Specific IPR and Specially Written Software 683](#_Toc189823809)

[Annex 2: Form Of Confidentiality Undertaking 684](#_Toc189823810)

[Schedule 28: Carbon Reduction 691](#_Toc189823811)

[Annex A: Optional Paragraphs 704](#_Toc189823812)

[Part A: General Provisions 704](#_Toc189823813)

[Part B: Sector Specific Paragraphs 705](#_Toc189823814)

[Schedule 29: Authority Specific Terms 711](#_Toc189823815)

Schedule 1

Definitions

# Schedule 1: Definitions

1. Definitions
   1. In the Contract, unless the context otherwise requires, capitalised expressions shall have the meanings set out in this Schedule 1 (*Definitions*) or the relevant Schedule in which that capitalised expression appears.
   2. If a capitalised expression does not have an interpretation in this Schedule or any other Schedule, it shall, in the first instance, be interpreted in accordance with the common interpretation within the relevant market sector/industry where appropriate. Otherwise, it shall be interpreted in accordance with the dictionary meaning.
   3. In the Contract, unless the context otherwise requires:
      1. the singular includes the plural and vice versa;
      2. reference to a gender includes the other gender and the neuter;
      3. references to a person include an individual, company, body corporate, corporation, unincorporated association, firm, partnership or other legal entity or Crown Body;
      4. a reference to a Law includes a reference to that Law as modified, amended, extended, consolidated, replaced or re-enacted (including as a consequence of the Retained EU Law (Revocation and Reform) Act 2023) from time to time before or after the date of this Contract and any prior or subsequent legislation under it;
      5. the words “**including**”, “**other**”, “**in particular**”, “**for example**” and similar words shall not limit the generality of the preceding words and shall be construed as if they were immediately followed by the words “**without limitation**”;
      6. references to “**writing**” include typing, printing, lithography, photography, display on a screen, electronic and facsimile transmission and other modes of representing or reproducing words in a visible form, and expressions referring to writing shall be construed accordingly;
      7. references to “**representations**” shall be construed as references to present facts, to “**warranties**” as references to present and future facts and to “**undertakings”** as references to obligations under the Contract;
      8. references to **“Clauses”** and **“Schedules”** are, unless otherwise provided, references to the clauses and schedules of the Core Terms and references in any Schedule to parts, paragraphs, annexes and tables are, unless otherwise provided, references to the parts, paragraphs, annexes and tables of the Schedule in which these references appear;
      9. references to **“Paragraphs”** are, unless otherwise provided, references to the paragraph of the appropriate Schedules unless otherwise provided; and
      10. references to a series of Clauses or Paragraphs shall be inclusive of the clause numbers specified;
      11. the headings in the Contract are for ease of reference only and shall not affect the interpretation or construction of the Contract;
      12. where the Authority is a Crown Body the Supplier shall be treated as contracting with the Crown as a whole;
      13. a reference to a document (including this Contract) is to that document as varied, amended, novated, ratified or replaced from time to time; and
      14. any monetary sums set out in this Contract shall (unless expressly stated otherwise) be in pounds sterling.
   4. Any reference in this Contract which immediately before IP Completion Day (or such later date when relevant EU law ceases to have effect pursuant to Section 1A of the European Union (Withdrawal) Act 2018) is a reference to (as it has effect from time to time):
      1. any EU regulation, EU decision, EU tertiary legislation or provision of the EEA agreement (“**EU References**”) which is to form part of domestic law by application of Section 3 of the European Union (Withdrawal) Act 2018 shall be read on and after IP Completion Day as a reference to the EU References as they form part of domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 as modified by domestic law from time to time; and
      2. any EU institution or EU authority or other such EU body shall be read on and after IP Completion Day as a reference to the UK institution, authority or body to which its functions were transferred.
   5. Where a standard, policy or document is referred to in this Contract by reference to a hyperlink, then if the hyperlink is changed or no longer provides access to the relevant standard, policy or document, the Supplier shall notify the Authority and the Parties shall update this Contract with a reference to the replacement hyperlink.

|  |  |
| --- | --- |
| “Accounting Reference Date” | in each year the date to which the Supplier prepares its annual audited financial statements; |
| “Achieve” | 1. in respect of a Test, to successfully pass a Test without any Test Issues; and 2. in respect of a Milestone, the issue of a Milestone Achievement Certificate in respect of that Milestone in accordance with the provisions of Schedule 10 (*Testing Procedures*),   and “Achieved” and “Achievement” shall be construed accordingly; |
| “Affected Party” | the Party seeking to claim relief in respect of a Force Majeure Event; |
| “Affiliate” | in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control with, that body corporate from time to time; |
| “Allowable Assumptions” | the assumptions set out in Annex 5 of Schedule 11 (*Charges and Invoicing*); |
| “Allowable Price” | in relation to the Retained Deliverables relating to a CPP Milestone, if any, an amount determined in accordance with the formula:  A – B  where:   1. A is an amount equal to the Costs incurred by the Supplier in providing or developing the relevant Retained Deliverables as reflected in the Financial Model together with an amount equal to the Anticipated Contract Life Profit Margin thereon; and 2. B is an amount equal to the Allowable Price Adjustment relating to the relevant Retained Deliverables, if any, or if there is no such Allowable Price Adjustment, zero,   provided that the Allowable Price for any Retained Deliverables shall in no circumstances exceed the aggregate amount of the Milestone Payments paid to the Supplier in respect of the Milestones (or in the case of Partial Termination, the Milestones for the parts of the Services terminated) relating to that CPP Milestone; |
| “Allowable Price Adjustment” | has the meaning given in Clause 32.9.3 (*Payments by the Supplier*); |
| “Annual Contract Report” | has the meaning given in Schedule 15 (*Financial Reports and Audit Rights*); |
| “Annual Revenue” | for the purposes of determining whether an entity is a Public Sector Dependent Supplier, the audited consolidated aggregate revenue (including share of revenue of joint ventures and Associates) reported by the Supplier or, as appropriate, the Supplier Group in its most recent published accounts, subject to the following methodology:   1. figures for accounting periods of other than 12 months should be scaled pro rata to produce a proforma figure for a 12 month period; and 2. where the Supplier, the Supplier Group and/or their joint ventures and Associates report in a foreign currency, revenue should be converted to British Pound Sterling at the closing exchange rate on the Accounting Reference Date; |
| “Anticipated Contract Life Profit Margin” | has the meaning given in Schedule 11 (*Charges and Invoicing*); |
| “Approved Sub‑Licensee” | any of the following:   1. a Crown Body; 2. any third party providing services to a Crown Body; and/or 3. any body (including any private sector body) which performs or carries on any of the functions and/or activities that previously had been performed and/or carried on by the Authority; |
| “Assets” | all assets and rights used by the Supplier to provide the Services in accordance with this Contract but excluding the Authority Assets; |
| “Associated Person” | has the meaning given to it in Section 44(4) of the Criminal Finances Act 2017; |
| “Associates” | in relation to an entity, an undertaking in which the entity owns, directly or indirectly, between 20% and 50% of the voting rights and exercises a degree of control sufficient for the undertaking to be treated as an associate under generally accepted accounting principles; |
| “Assurance” | written confirmation from a Relevant Authority to the Supplier that the CRP Information is approved by the Relevant Authority; |
| “ATP Milestone” | the Milestone linked to Authority to Proceed for the relevant Operational Services set out in the Implementation Plan; |
| “Audit” | any exercise by the Authority of its Audit Rights pursuant to Clause 12 (*Records, Reports, Audit and Open Book Data*) and Schedule 15 (*Financial Reports and Audit Rights*); |
| “Audit Agents” | 1. the Authority’s internal and external auditors; 2. the Authority’s statutory or regulatory auditors; 3. the Comptroller and Auditor General, their staff and/or any appointed representatives of the National Audit Office; 4. HM Treasury or the Cabinet Office; 5. any party formally appointed by the Authority to carry out audit or similar review functions; and 6. successors or assigns of any of the above; |
| “Audit Rights” | the audit and access rights referred to in Schedule 15 (*Financial Reports and Audit Rights*); |
| “Authority Assets” | the Authority Materials, the Authority infrastructure and any other data, software, assets, equipment or other property owned by and/or licensed or leased to the Authority and which is or may be used in connection with the provision or receipt of the Services; |
| “Authority Background IPRs” | 1. IPRs owned by the Authority before the Effective Date, including IPRs contained in any of the Authority’s Know‑How, documentation, processes and procedures; 2. IPRs created by the Authority independently of this Contract; and/or 3. Crown Copyright which is not available to the Supplier otherwise than under this Contract;   but excluding IPRs owned by the Authority subsisting in the Authority Software; |
| “Authority Cause” | any material breach by the Authority of any of the Authority Responsibilities, except to the extent that such breach is:   1. the result of any act or omission by the Authority to which the Supplier has given its prior consent; or 2. caused by the Supplier, any Sub-contractor or any Supplier Personnel; |
| "Authority Equipment" | any hardware, computer or telecoms devices, and equipment that forms part of the Authority System; |
| “Authority IT Strategy” | the Authority’s IT policy in force as at the Effective Date (a copy of which has been supplied to the Supplier), as updated from time to time in accordance with the Change Control Procedure; |
| “Authority Materials” | the Government Data together with any materials, documentation, information, programs and codes supplied by the Authority to the Supplier, the IPRs in which:   1. are owned or used by or on behalf of the Authority; and 2. are or may be used in connection with the provision or receipt of the Services,   but excluding any Project Specific IPRs, Specially Written Software, Supplier Software, Third Party Software and Documentation relating to Supplier Software or Third Party Software; |
| “Authority Premises” | premises owned, controlled or occupied by the Authority and/or any Crown Body which are made available for use by the Supplier or its Sub-contractors for provision of the Services (or any of them); |
| “Authority Representative” | the representative appointed by the Authority pursuant to Clause 11.4 (*Representatives*); |
| “Authority Requirements” | the requirements of the Authority set out in Schedule 2 (*Services Description*), Schedule 3 (*Performance Levels*) Schedule 4 (*Standards*), Schedule 5 (*Security Management*), Schedule 6 (*Insurance Requirements*) Schedule 9 (*Implementation Plan*), Schedule 20 (*Reports and Records Provisions*), Schedule 21 (*Exit Management*) and Schedule 22 (*Service Continuity Plan and Corporate Resolution Planning*); |
| “Authority Responsibilities” | the responsibilities of the Authority specified in Schedule 7 (*Authority Responsibilities*); |
| “Authority Software” | software which is owned by or licensed to the Authority (other than under or pursuant to this Contract) and which is or will be used by the Supplier for the purposes of providing the Services; |
| “Authority System” | the Authority's information and communications technology system, including any software or Authority Equipment, owned by the Authority or leased or licenced to it by a third party, that:  (a) is used by the Authority or the Supplier in connection with this Contract;  (b) interfaces with the Supplier System; and/or  (c) is necessary for the Authority to receive the Services; |
| “Authority to Proceed” or “ATP” | the authorisation to the Supplier to commence the provision of the relevant Operational Services to the Authority, provided by the Authority in the form of a Milestone Achievement Certificate in respect of the ATP Milestone; |
| “Balanced Sustainablity Report” | has the meaning given in Paragraph 1.1.2 of Part B of Schedule 3 (*Performance Levels*); |
| “Board” | the Supplier’s board of directors; |
| “Board Confirmation” | the written confirmation from the Board in accordance with Paragraph 8 of Schedule 14 (*Financial Distress*); |
| “Breakage Costs Payment” | has the meaning given in Schedule 12 (*Payments on Termination*); |
| “Cabinet Office Markets and Suppliers Team” | the UK Government’s team responsible for managing the relationship between government and its Strategic Suppliers, or any replacement or successor body carrying out the same function; |
| “Certificate of Costs” | has the meaning given in Schedule 11 (*Charges and Invoicing*); |
| “Change” | any change to this Contract; |
| “Change Authorisation Note” | a form setting out an agreed Contract Change which shall be substantially in the form of Annex 2: Change Authorisation Note of Schedule 18 (*Change Control Procedure*); |
| “Change Control Procedure” | the procedure for changing this Contract set out in Schedule 18 (*Change Control Procedure*); |
| “Change in Law” | any change in Law which impacts on the performance of the Services which comes into force after the Effective Date; |
| “Change Request” | a written request for a Contract Change substantially in the form of 1 (*Change Request Form*) of Schedule 18 (*Change Control Procedure*)*;* |
| “Charges” | the charges for the provision of the Services set out in or otherwise calculated in accordance with Schedule 11 (*Charges and Invoicing*), including any Milestone Payment or Service Charge; |
| “Class 1 Transaction” | has the meaning set out in the listing rules issued by the UK Listing Authority; |
| “CNI” | Critical National Infrastructure; |
| "Code" | in respect of the Developed System:   1. the source code; 2. the object code; 3. third party components, including third party coding frameworks and libraries; and 4. all supporting documentation; |
| “Commercially Sensitive Information” | the information listed in section 5 *(Commercially Sensitive Information)* of the Front Sheet comprising the information of a commercially sensitive nature relating to:   1. the pricing of the Services; 2. details of the Supplier’s IPRs; and 3. the Supplier’s business and investment plans;   which the Supplier has indicated to the Authority that, if disclosed by the Authority, would cause the Supplier significant commercial disadvantage or material financial loss; |
| “Comparable Supply” | the supply of services to another customer of the Supplier that are the same or similar to any of the Services; |
| “Compensation for Unacceptable KPI Failure” | has the meaning given in Clause 7.4.1 (*Unacceptable KPI Failure*); |
| “Compensation Payment” | has the meaning given in Schedule 12 (*Payments on Termination*); |
| “Confidential Information” | 1. Information, including all Personal Data, which (however it is conveyed) is provided by the Disclosing Party pursuant to or in anticipation of this Contract that relates to:    1. the Disclosing Party Group; or    2. the operations, business, affairs, developments, intellectual property rights, trade secrets, know-how and/or personnel of the Disclosing Party Group; 2. other Information provided by the Disclosing Party pursuant to or in anticipation of this Contract that is clearly designated as being confidential or equivalent or that ought reasonably to be considered to be confidential (whether or not it is so marked) which comes (or has come) to the Recipient’s attention or into the Recipient’s possession in connection with this Contract; 3. discussions, negotiations, and correspondence between the Disclosing Party or any of its directors, officers, employees, consultants or professional advisers and the Recipient or any of its directors, officers, employees, consultants and professional advisers in connection with this Contract and all matters arising therefrom; and 4. Information derived from any of the above,   but not including any Information which:   * 1. was in the possession of the Recipient without obligation of confidentiality prior to its disclosure by the Disclosing Party;   2. the Recipient obtained on a non-confidential basis from a third party who is not, to the Recipient’s knowledge or belief, bound by a confidentiality agreement with the Disclosing Party or otherwise prohibited from disclosing the information to the Recipient;   3. was already generally available and in the public domain at the time of disclosure otherwise than by a breach of this Contract or breach of a duty of confidentiality;   4. was independently developed without access to the Confidential Information; or   5. relates to the Supplier’s:      1. performance under this Contract; or      2. failure to pay any Sub-contractor as required pursuant to Clause 15.13.1 (*Supply Chain Protection*); |
| “Conflict of Interest” | a direct or indirect conflict between the financial, professional or personal interests of the Supplier or the Supplier Personnel and the duties owed to the Authority under the Contract, in the reasonable opinion of the Authority; |
| “Contract” | the contract between the Authority and the Supplier; |
| “Contract Change” | any change to this Contract other than an Operational Change; |
| “Contract Inception Report” | the initial financial model in a form agreed by the Supplier and the Authority in writing on or before the Effective Date; |
| “Contract Year” | 1. a period of 12 months commencing on the Effective Date; or 2. thereafter a period of 12 months commencing on each anniversary of the Effective Date;   provided that the final Contract Year shall end on the expiry or termination of the Term; |
| “Control” | the possession by person, directly or indirectly, of the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and “Controls” and “Controlled” shall be interpreted accordingly; |
| “Controller” | has the meaning given in the UK GDPR or the EU GDPR as the context requires; |
| “Corporate Change Event” | 1. any change of Control of the Supplier or a Parent Undertaking of the Supplier; 2. any change of Control of any member of the Supplier Group which, in the reasonable opinion of the Authority, could have a material adverse effect on the Services; 3. any change to the business of the Supplier or any member of the Supplier Group which, in the reasonable opinion of the Authority, could have a material adverse effect on the Services; 4. a Class 1 Transaction taking place in relation to the shares of the Supplier or any Parent Undertaking of the Supplier whose shares are listed on the main market of the London Stock Exchange plc; 5. an event that could reasonably be regarded as being equivalent to a Class 1 Transaction taking place in respect of the Supplier or any Parent Undertaking of the Supplier; 6. payment of dividends by the Supplier or the ultimate Parent Undertaking of the Supplier Group exceeding 25% of the Net Asset Value of the Supplier or the ultimate Parent Undertaking of the Supplier Group respectively in any 12 month period; 7. an order is made or an effective resolution is passed for the winding up of any member of the Supplier Group; 8. any member of the Supplier Group stopping payment of its debts generally or becoming unable to pay its debts within the meaning of section 123(1) of the Insolvency Act 1986 or any member of the Supplier Group ceasing to carry on all or substantially all its business, or any compromise, composition, arrangement or agreement being made with creditors of any member of the Supplier Group; 9. the appointment of a receiver, administrative receiver or administrator in respect of or over all or a material part of the undertaking or assets of any member of the Supplier Group; and/or 10. any process or events with an effect analogous to those in Paragraphs (e) to (g) inclusive above occurring to a member of the Supplier Group in a jurisdiction outside England and Wales; |
| “Corporate Change Event Grace Period” | a grace period agreed to by the Relevant Authority for providing CRP Information and/or updates to Service Continuity Plan after a Corporate Change Event |
| “Corporate Resolvability Assessment (Structural Review)” | part of the CRP Information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraphs 2 and Annex 2: Corporate Resolvability Assessment (Structural Review) of Schedule 22 (*Service Continuity Plan and Corporate Resolution Planning*); |
| “Costs” | has the meaning given in Schedule 11 (*Charges and Invoicing*); |
| “CPP Milestone” | a contract performance point as set out in the Implementation Plan, being the Milestone at which the Supplier has demonstrated that the Supplier Solution or relevant Service is working satisfactorily in its operating environment in accordance with Schedule 10 (*Testing Procedures*); |
| “Critical National Infrastructure” | those critical elements of UK national infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:   1. major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or 2. significant impact on the national security, national defence, or the functioning of the UK; |
| “Critical Performance Failure” | 1. the Supplier accruing in aggregate **[insert** number] or more Service Points (in terms of the number of points allocated) in any period of **[insert** number] months; or 2. the Supplier accruing Service Credits or Compensation for Unacceptable KPI Failure which meet or exceed the Service Credit Cap; |
| “Critical Service Contract” | the overall status of the Services provided under this Contract as determined by the Authority and specified in section 9 *(Corporate Resolution Planning)* of the Front Sheet; |
| “Crown Body” | the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Government and the Welsh Government), including government ministers and government departments and particular bodies, persons, commissions or agencies from time to time carrying out functions on its behalf; |
| “Crown Copyright” | has the meaning given in the Copyright, Designs and Patents Act 1988 |
| “CRP Information” | the Corporate Resolution Planning Information, together being the:   1. Exposure Information (Contracts List); 2. Corporate Resolvability Assessment (Structural Review); and 3. Financial Information and Commentary; |
| “CRTPA” | the Contracts (Rights of Third Parties) Act 1999; |
| “Data Loss Event” | any event that results, or may result, in unauthorised access to Personal Data held by the Supplier under this Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach; |
| “Data Protection Impact Assessment” | an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data; |
| “Data Protection Legislation” | 1. the UK GDPR; 2. the DPA 2018 to the extent that it relates to Processing of personal data and privacy; 3. all applicable Law about the processing of personal data and privacy; and 4. (to the extent that it applies) the EU GDPR; |
| “Data Subject” | has the meaning given to it in the UK GDPR or the EU GDPR as the context requires; |
| “Data Subject Request” | a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to their Personal Data; |
| “Deductions” | all Service Credits, Compensation for Unacceptable KPI Failure, Delay Payments or any other deduction which is paid or payable to the Authority under this Contract; |
| “Default” | any breach of the obligations of the relevant Party (including abandonment of this Contract in breach of its terms, repudiatory breach or breach of a fundamental term) or any other default, act, omission, negligence or statement:   1. in the case of the Authority, of its employees, servants, agents; or 2. in the case of the Supplier, of its Sub-contractors or any Supplier Personnel,   in connection with or in relation to the subject-matter of this Contract and in respect of which such Party is liable to the other; |
| “Defect” | 1. any error, damage or defect in the manufacturing of a Deliverable; or 2. any error or failure of code within the Software which causes a Deliverable to malfunction or to produce unintelligible or incorrect results; or 3. any failure of any Deliverable to provide the performance, features and functionality specified in the Authority Requirements or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from meeting its associated Test Success Criteria; or 4. any failure of any Deliverable to operate in conjunction with or interface with any other Deliverable in order to provide the performance, features and functionality specified in the Authority Requirements or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from meeting its associated Test Success Criteria; |
| “Delay” | 1. a delay in the Achievement of a Milestone by its Milestone Date; or 2. a delay in the design, development, testing or implementation of a Deliverable by the relevant date set out in the Implementation Plan; |
| “Delay Deduction Period” | the period of one hundred (100) days commencing on the relevant Milestone Date; |
| “Delay Payments” | the amounts payable by the Supplier to the Authority in respect of a Delay in Achieving a Key Milestone as specified in Schedule 11 (*Charges and Invoicing*); |
| “Deliverable” | an item, feature or software delivered or to be delivered by the Supplier at or before a Milestone Date or at any other stage during the performance of this Contract; |
| “Dependent Parent Undertaking” | any Parent Undertaking which provides any of its Subsidiary Undertakings and/or Associates, whether directly or indirectly, with any financial, trading, managerial or other assistance of whatever nature, without which the Supplier would be unable to continue the day to day conduct and operation of its business in the same manner as carried on at the time of entering into this Contract, including for the avoidance of doubt the provision of the Services in accordance with the terms of this Contract; |
| “Detailed Implementation Plan” | the plan developed and revised from time to time in accordance with Paragraphs 3 and 4 of Schedule 9 (*Implementation Plan*); |
| "Developed System" | any software or system that the Supplier is required to develop under this Contract either:  (a) as part of the Services; or  (b) as a requirement or part of a requirement to create or modify Software to:  (i) provide the Services; or  (ii) Handle Government Data; |
| “Disclosing Party” | has the meaning given in Clause 19.1 (*Confidentiality*); |
| “Disclosing Party Group” | 1. where the Disclosing Party is the Supplier, the Supplier and any Affiliates of the Supplier; and 2. where the Disclosing Party is the Authority, the Authority and any Crown Body with which the Authority or the Supplier interacts in connection with this Contract; |
| “Dispute” | any dispute, difference or question of interpretation arising out of or in connection with this Contract, including any dispute, difference or question of interpretation relating to the Services, failure to agree in accordance with the Change Control Procedure or any matter where this Contract directs the Parties to resolve an issue by reference to the Dispute Resolution Procedure; |
| “Dispute Notice” | a written notice served by one Party on the other stating that the Party serving the notice believes that there is a Dispute; |
| “Dispute Resolution Procedure” | the dispute resolution procedure set out in Schedule 19 (*Dispute Resolution Procedure*); |
| “Documentation” | descriptions of the Services and Performance Indicators, details of the Supplier System (including (i) vendors and versions for off-the-shelf components and (ii) source code and build information for proprietary components), relevant design and development information, technical specifications of all functionality including those not included in standard manuals (such as those that modify system performance and access levels), configuration details, test scripts, user manuals, operating manuals, process definitions and procedures, and all such other documentation as:   1. is required to be supplied by the Supplier to the Authority under this Contract; 2. would reasonably be required by a competent third party capable of Good Industry Practice contracted by the Authority to develop, configure, build, deploy, run, maintain, upgrade and test the individual systems that provide Services; 3. is required by the Supplier in order to provide the Services; and/or 4. has been or shall be generated for the purpose of providing the Services; |
| “DPA 2018” | the Data Protection Act 2018; |
| “Due Diligence Information” | any information supplied to the Supplier by or on behalf of the Authority prior to the Effective Date; |
| “EEA” | European Economic Area |
| “Effective Date” | the later of:   1. the date on which this Contract is signed by both Parties; and 2. the date on which the Condition Precedent has been satisfied or waived in accordance with Clause 4.2 (*Condition Precedent*) (if Clause 4.2 applies pursuant to section 9 *(Optional Schedules)* of the Front Sheet); |
| “EIRs” | the Environmental Information Regulations 2004, together with any guidance and/or codes of practice issued by the Information Commissioner or any Crown Body in relation to such Regulations; |
| “Emergency Maintenance” | ad hoc and unplanned maintenance provided by the Supplier where:   1. the Authority reasonably suspects that the IT Environment or the Services, or any part of the IT Environment or the Services, has or may have developed a fault, and notifies the Supplier of the same; or 2. the Supplier reasonably suspects that the IT Environment or the Services, or any part the IT Environment or the Services, has or may have developed a fault; |
| “Employee Liabilities” | all claims, actions, proceedings, orders, demands, complaints, investigations (save for any claims for personal injury which are covered by insurance) and any award, compensation, damages, tribunal awards, fine, loss, order, penalty, disbursement, payment made by way of settlement and costs, expenses and legal costs reasonably incurred in connection with a claim or investigation related to employment including in relation to the following:   1. redundancy payments including contractual or enhanced redundancy costs, termination costs and notice payments; 2. unfair, wrongful or constructive dismissal compensation; 3. compensation for discrimination on grounds of sex, race, disability, age, religion or belief, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation or claims for equal pay; 4. compensation for less favourable treatment of part-time workers or fixed term employees; 5. outstanding employment debts and unlawful deduction of wages including any PAYE and national insurance contributions; 6. employment claims whether in tort, contract or statute or otherwise; 7. any investigation relating to employment matters by the Equality and Human Rights Commission or other enforcement, regulatory or supervisory body and of implementing any requirements which may arise from such investigation; |
| “Employment Regulations” | the Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) as amended or replaced; |
| “Estimated Year 1 Charges” | the estimated Charges payable by the Authority during the first Contract Year, as set out in the Financial Model; |
| “Estimated Initial Service Charges” | the estimated Service Charges payable by the Authority during the period of 12 months from the first Operational Service Commencement Date, as set out in the Financial Model; |
| “EU GDPR” | Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of personal data and on the free movement of such data (General Data Protection Regulation) as it has effect in EU law; |
| “EU” | European Union; |
| “Exit Management” | services, activities, processes and procedures to ensure a smooth and orderly transition of all or part of the Services from the Supplier to the Authority and/or a Replacement Supplier, as set out or referred to in Schedule 21 (*Exit Management*); |
| “Exit Plan” | the plan produced and updated by the Supplier during the Term in accordance with Paragraph 4 of Schedule 21 (*Exit Management*); |
| “Expedited Dispute Timetable” | the reduced timetable for the resolution of Disputes set out in Paragraph 3 of Schedule 19 (*Dispute Resolution Procedure*); |
| “Expert” | has the meaning given in Schedule 19 (*Dispute Resolution Procedure*); |
| “Expert Determination” | the process described in Paragraph 6 of Schedule 19 (*Dispute Resolution Procedure*); |
| “Exposure Information (Contracts List)” | part of the CRP Information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraph 2 and Annex 1 of Part B of Schedule 22 (*Service Continuity Plan and Corporate Resolution Planning*); |
| “Extension Period” | has the meaning given in section 3 *(Contract Particulars)* of the Front Sheet; |
| "Final Supplier Personnel List" | has the meaning given in Schedule 24 (*Staff Transfer*); |
| “Financial Distress Event” | the occurrence of one or more of the events listed in Paragraph 3.1 of Schedule 14 (*Financial Distress*); |
| “Financial Information and Commentary” | part of the CRP Information requirements set out in accordance with Paragraph 2 and Annex 3 of Part B of Schedule 22 (*Service Continuity Plan and Corporate Resolution Planning*); |
| “Financial Distress Remediation Plan” | a plan setting out how the Supplier will ensure the continued performance and delivery of the Services in accordance with this Contract in the event that a Financial Distress Event occurs. This plan should include what the Authority would need to put in place to ensure performance and delivery of the Services in accordance with this Contract up to and including any Insolvency Event in respect of the relevant FDE Group entity and may refer to the Insolvency Continuity Plan in this regard; |
| “Financial Model” | has the meaning given in Schedule 15 (*Financial Reports and Audit Rights*); |
| “Financial Reports” | has the meaning given in Schedule 15 (*Financial Reports and Audit Rights*); |
| “Financial Transparency Objectives” | has the meaning given in Schedule 15 (*Financial Reports and Audit Rights*); |
| "Find a Tender Service" | the online government portal which allows suppliers to search for information about contracts as prescribed the Procurement Act 2023; |
| “FOIA” | the Freedom of Information Act 2000 and any subordinate legislation made under that Act from time to time, together with any guidance and/or codes of practice issued by the Information Commissioner or any relevant Crown Body in relation to such Act; |
| “Force Majeure Event” | any event outside the reasonable control of either Party affecting its performance of its obligations under this Contract arising from acts, events, omissions, happenings or non-happenings beyond its reasonable control and which are not attributable to any wilful act, neglect or failure to take reasonable preventative action by that Party, including riots, war or armed conflict, acts of terrorism, acts of government, local government or regulatory bodies, fire, flood, storm or earthquake, or other natural disaster but excluding any industrial dispute relating to the Supplier or the Supplier Personnel or any other failure in the Supplier’s or a Sub-contractor’s supply chain; |
| “Force Majeure Notice” | a written notice served by the Affected Party on the other Party stating that the Affected Party believes that there is a Force Majeure Event; |
| “Former Supplier” | has the meaning given in Schedule 24 (*Staff Transfer*); |
| "Front Sheet" | the 'front sheet' included at the front of this Contract containing certain particulars of the Contract; |
| “General Change in Law” | a Change in Law where the change is of a general legislative nature (including taxation or duties of any sort affecting the Supplier) or which affects or relates to a Comparable Supply; |
| “Good Industry Practice” | at any time the exercise of that degree of care, skill, diligence, prudence, efficiency, foresight and timeliness which would be reasonably expected at such time from a leading and expert supplier of services similar to the Services to a customer like the Authority, such supplier seeking to comply with its contractual obligations in full and complying with applicable Laws; |
| “Goods” | has the meaning given in Clause 9.7 (*Supply of Goods*); |
| "Government Data" | any:  (a) data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media;  (b) Personal Data for which the Authority is a, or the, Data Controller; or  (c) any meta data relating to categories of data referred to in paragraphs (a) or (b);  that:  (i) is supplied to the Supplier by or on behalf of the Authority; or  (ii) the Supplier is required to generate, Process, Handle, store or transmit under this Contract; and  for the avoidance of doubt includes the Code and any meta data relating to the Code; |
| “Guarantee” | where the Authority has selected Schedule 25 (*Guarantee*) in section 3 of the Front Sheet, the deed of guarantee in favour of the Authority entered into by the Guarantor on or about the date of this Contract (which is in the form set out in Schedule 25 *(Guarantee)*), or any guarantee acceptable to the Authority that replaces it from time to time; |
| “Guarantor” | **[insert** name], a company registered in **[insert** country] with company number **[insert** company number] and whose registered office is at **[insert** registered address]; |
| "Handle" | any operation performed on data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of that data; |
| “Health and Safety Policy” | the health and safety policy of the Authority and/or other relevant Crown Body as provided to the Supplier on or before the Effective Date and as subsequently provided to the Supplier from time to time except any provision of any such subsequently provided policy that cannot be reasonably reconciled to ensuring compliance with applicable Law regarding health and safety; |
| “HMRC” | HM Revenue & Customs; |
| “Impact Assessment” | has the meaning given in Schedule 18 (*Change Control Procedure*); |
| “Implementation Plan” | the Outline Implementation Plan or (if and when approved by the Authority pursuant to Paragraph 3 of Schedule 9 (*Implementation Plan*)) the Detailed Implementation Plan as updated in accordance with Paragraph 4 of Schedule 9 (*Implementation Plan*) from time to time; |
| “Implementation Services” | the implementation services described as such in the Services Description; |
| “Implementation Services Commencement Date” | the date on which the Supplier is to commence provision of the first of the Services, being **[insert** date]; |
| “Indemnified Person” | the Authority and each and every person to whom the Authority (or any direct or indirect sub-licensee of the Authority) sub-licenses, assigns or novates any Relevant IPRs or rights in Relevant IPRs in accordance with this Contract; |
| “Independent Controller” | a party which is Controller of the same Personal Data as the other Party and there is no element of joint control with regards to that Personal Data; |
| “Information” | all information of whatever nature, however conveyed and in whatever form, including in writing, orally, by demonstration, electronically and in a tangible, visual or machine-readable medium (including CD-ROM, magnetic and digital form); |
| “Initial Term” | has the meaning given in section 3 *(Contract Particulars)* of the Front Sheet; |
| “Initial Upload Date” | the occurrence of an event detailed in Schedule 20 (*Reports and Records Provisions*) Annex 2: Records *To Upload To Virtual Library*) which requires the Supplier to provide its initial upload of the relevant information to the Virtual Library; |
| “Insolvency Event” | with respect to any person, means:   1. that person suspends, or threatens to suspend, payment of its debts, or is unable to pay its debts as they fall due or admits inability to pay its debts, or:    1. (being a company or a LLP) is deemed unable to pay its debts within the meaning of section 123 of the Insolvency Act 1986, or    2. (being a partnership) is deemed unable to pay its debts within the meaning of section 222 of the Insolvency Act 1986; 2. that person commences negotiations with one or more of its creditors (using a voluntary arrangement, scheme of arrangement or otherwise) with a view to rescheduling any of its debts, or makes a proposal for or enters into any compromise or arrangement with one or more of its creditors or takes any step to obtain a moratorium pursuant to Section 1A and Schedule A1 of the Insolvency Act 1986 other than (in the case of a company, a LLP or a partnership) for the sole purpose of a scheme for a solvent amalgamation of that person with one or more other companies or the solvent reconstruction of that person; 3. another person becomes entitled to appoint a receiver over the assets of that person or a receiver is appointed over the assets of that person; 4. a creditor or encumbrancer of that person attaches or takes possession of, or a distress, execution or other such process is levied or enforced on or sued against, the whole or any part of that person’s assets and such attachment or process is not discharged within fourteen (14) days; 5. that person suspends or ceases, or threatens to suspend or cease, carrying on all or a substantial part of its business; 6. where that person is a company, a LLP or a partnership:    1. a petition is presented (which is not dismissed within fourteen (14) days of its service), a notice is given, a resolution is passed, or an order is made, for or in connection with the winding up of that person other than for the sole purpose of a scheme for a solvent amalgamation of that person with one or more other companies or the solvent reconstruction of that person;    2. an application is made to court, or an order is made, for the appointment of an administrator, or if a notice of intention to appoint an administrator is filed at Court or given or if an administrator is appointed, over that person;    3. (being a company or a LLP) the holder of a qualifying floating charge over the assets of that person has become entitled to appoint or has appointed an administrative receiver; or    4. (being a partnership) the holder of an agricultural floating charge over the assets of that person has become entitled to appoint or has appointed an agricultural receiver; or 7. any event occurs, or proceeding is taken, with respect to that person in any jurisdiction to which it is subject that has an effect equivalent or similar to any of the events mentioned above; |
| “Intellectual Property Rights” or “IPRs” | 1. copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in Internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information; 2. applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction; and 3. all other rights having equivalent or similar effect in any country or jurisdiction; |
| “Intervention Cause” | has the meaning given in Clause 27.1 (*Remedial Adviser*); |
| “Intervention Notice” | has the meaning given in Clause 27.1 (*Remedial Adviser*); |
| “Intervention Period” | has the meaning given in Clause 27.2.3 (*Remedial Adviser*); |
| “Intervention Trigger Event” | 1. any event falling within limb (a), (b), (c), (e), (f) or (g) of the definition of a Supplier Termination Event; 2. a Default by the Supplier that is materially preventing or materially delaying the performance of the Services or any material part of the Services; 3. the Supplier accruing in aggregate **[insert** number of points which is 75% of the points that would constitute a “Critical Performance Failure”] or more Service Points (in terms of the number of points allocated) in any period of **[insert** number of months taken from definition of “Critical Performance Failure”] months; 4. the Supplier accruing Service Credits which meet or exceed 75% of the Service Credit Cap; and/or 5. the Supplier not Achieving a Key Milestone within seventy-five (75) days of its relevant Milestone Date; |
| “IP Completion Day” | has the meaning given to it in the European Union (Withdrawal Agreement) Act 2020; |
| “IPRs Claim” | any claim against any Indemnified Person of infringement or alleged infringement (including the defence of such infringement or alleged infringement) of any Relevant IPRs save for any such claim to the extent that it is caused by any use by or on behalf of that Indemnified Person of any Relevant IPRs, or the use of the Authority Software by or on behalf of the Supplier, in either case in combination with any item not supplied or recommended by the Supplier pursuant to this Contract or for a purpose not reasonably to be inferred from the Services Description or the provisions of this Contract; |
| "IR35" | Chapter 8 and Chapter 10 of Part 2 of Income Tax (Earnings and Pensions) Act 2003 and the Social Security Contributions (Intermediaries) Regulations 2000; |
| “IT” | information and communications technology; |
| “IT Environment” | the Authority System and the Supplier System; |
| “Joint Controllers” | has the meaning given in Article 26 of the UK GDPR, or EU GDPR, as the context requires; |
| “Key Milestone” | the Milestones identified in the Implementation Plan as key milestones and in respect of which Delay Payments may be payable in accordance with Paragraph 1 of Part C of Schedule 11 (*Charges and Invoicing*) if the Supplier fails to Achieve the Milestone Date in respect of such Milestone; |
| “Key Performance Indicator” | the key performance indicators set out in Table 1 of Part A of Annex 1 of Schedule 3 (*Performance Levels*); |
| “Key Personnel” | those persons appointed by the Supplier to fulfil the Key Roles, being the persons listed in section 11 *(Key Personnel)* of the Front Sheet against each Key Role as at the Effective Date or as amended from time to time in accordance with Clauses 14.5 and 14.6 (*Key Personnel*); |
| “Key Roles” | a role described as a Key Role in section 11 *(Key Personnel)* of the Front Sheet and any additional roles added from time to time in accordance with Clause 14.4 (*Key Personnel*); |
| “Key Sub-contract” | each Sub-contract with a Key Sub-contractor; |
| “Key Sub-contractor” | any Sub-contractor:   1. which, in the opinion of the Authority, performs (or would perform if appointed) a critical role in the provision of all or any part of the Services; and/or 2. with a Sub-contract with a contract value which at the time of appointment exceeds (or would exceed if appointed) 10% of the aggregate Charges forecast to be payable under this Contract (as set out in the Financial Model); |
| “Know-How” | all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know how relating to the Services but excluding know how already in the other Party’s possession before this Contract; |
| “KPI Failure” | a failure to meet the Target Performance Level in respect of a Key Performance Indicator; |
| “KPI Service Threshold” | shall be as set out against the relevant Key Performance Indicator in Table 1 of Part A of Annex 1 of Schedule 3 (*Performance Levels*); |
| “Law” | any law, statute, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, right within the meaning of the European Union (Withdrawal) Act 2018 as amended by European Union (Withdrawal Agreement) Act 2020, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements of any regulatory body with which the Supplier is bound to comply; |
| “LED” | Law Enforcement Directive (Directive (EU) 2016/680); |
| “Licensed Software” | all and any Software licensed by or through the Supplier, its Sub-contractors or any third party to the Authority for the purposes of or pursuant to this Contract, including any Supplier Software, Third Party Software and/or any Specially Written Software; |
| “Losses” | losses, liabilities, damages, costs and expenses (including legal fees on a solicitor/client basis) and disbursements and costs of investigation, litigation, settlement, judgment interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty or otherwise; |
| “Maintenance Schedule” | shall have the meaning set out in Clause 9.4 (*Maintenance*); |
| “Malicious Software” | any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence; |
| “Management Information” | the management information specified in Schedule 3 (*Performance Levels*), Schedule 11 (*Charges and Invoicing*) and Schedule 17 (*Governance*) to be provided by the Supplier to the Authority; |
| “Material KPI Failure” | 1. a Serious KPI Failure; 2. a Severe KPI Failure; or 3. a failure by the Supplier to meet a KPI Service Threshold; |
| “Material PI Failure” | 1. a failure by the Supplier to meet the PI Service Threshold in respect of 25% or more of the Subsidiary Performance Indicators that are measured in that Service Period; and/or 2. a failure by the Supplier to meet the Target Performance Level in respect of 50% or more of the Subsidiary Performance Indicators that are measured in that Service Period; |
| “Measurement Period” | in relation to a Key Performance Indicator or Subsidiary Performance Indicator, the period over which the Supplier’s performance is measured (for example, a Service Period if measured monthly or a 12 month period if measured annually); |
| “Milestone” | an event or task described in the Implementation Plan which, if applicable, shall be completed by the relevant Milestone Date; |
| “Milestone Achievement Certificate” | the certificate to be granted by the Authority when the Supplier has Achieved a Milestone, which shall be in substantially the same form as that set out in Annex 3 of Schedule 10 (*Testing Procedures*); |
| “Milestone Adjustment Payment Amount” | in respect of each CPP Milestone that is the subject of a Milestone Adjustment Payment Notice, an amount determined in accordance with the formula:  A – B  where:   1. A is an amount equal to the aggregate sum of all Milestone Payments paid to the Supplier in respect of the Milestones (or in the case of Partial Termination, the Milestones for the parts of the Services terminated) relating to that CPP Milestone; and 2. B is an amount equal to the aggregate Allowable Price for the Retained Deliverables relating to that CPP Milestone or, if there are no such Retained Deliverables, zero; |
| “Milestone Adjustment Payment Notice” | has the meaning given in Clause 32.8 (*Payments by the Supplier*); |
| “Milestone Date” | the target date set out against the relevant Milestone in the Implementation Plan by which the Milestone must be Achieved; |
| “Milestone Payment” | a payment identified in Schedule 11 (*Charges and Invoicing*) to be made following the issue of a Milestone Achievement Certificate; |
| “Milestone Retention” | has the meaning given in Schedule 11 (*Charges and Invoicing*); |
| “Minor KPI Failure” | shall be as set out against the relevant Key Performance Indicator in Table 1 of Part A of Annex 1 of Schedule 3 (*Performance Levels*); |
| [Optional: “Modern Slavery Assessment Tool”  [*Guidance: Include this definition if Optional Clause 33.8.13 is included in the Core Terms*] | the modern slavery risk identification and management tool which can be found online at: <https://supplierregistration.cabinetoffice.gov.uk/msat>] |
| “Month” | a calendar month and “monthly” shall be interpreted accordingly; |
| “Multi-Party Dispute Resolution Procedure” | has the meaning given in Paragraph 9.1 of Schedule 19 (*Dispute Resolution Procedure*); |
| “Multi-Party Procedure Initiation Notice” | has the meaning given in Paragraph 9.2 of Schedule 19 (*Dispute Resolution Procedure*); |
| “National Insurance” | contributions required by the Social Security Contributions and Benefits Act 1992 and made in accordance with the Social Security (Contributions) Regulations 2001 (SI 2001/1004); |
| “New Releases” | an item produced primarily to extend, alter or improve the Software and/or any Deliverable by providing additional functionality or performance enhancement (whether or not defects in the Software and/or Deliverable are also corrected) while still retaining the original designated purpose of that item; |
| “Non-trivial Customer Base” | a significant customer base with respect to the date of first release and the relevant market but excluding Affiliates and other entities related to the licensor; |
| “Non-retained Deliverables” | in relation to a CPP Milestone Payment Notice and each CPP Milestone the subject of that CPP Milestone Payment Notice, Deliverables provided to the Authority which relate to the relevant CPP Milestone(s) and which are not Retained Deliverables; |
| “Notifiable Default” | shall have the meaning given in Clause 25.1 (*Rectification Plan Process*); |
| “Object Code” | software and/or data in machine-readable, compiled object code form; |
| “Open Book Data” | has the meaning given in Schedule 15 (*Financial Reports and Audit Rights*); |
| “Open Licence” | any material that is published for use, with rights to access, copy and modify and publish, by any person for free, under a generally recognised open licence including Open Government Licence as set out at http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/ and the Open Standards Principles documented at <https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles> , and includes the Open Source publication of Software; |
| “Open Source” | computer Software that is released on the internet for use by any person, such release usually being made under a recognised open source licence and stating that it is released as open source; |
| “Operating Environment” | the Authority System and the Sites; |
| “Operational Change” | any change in the Supplier’s operational procedures which in all respects, when implemented:   1. will not affect the Charges and will not result in any other costs to the Authority; 2. may change the way in which the Services are delivered but will not adversely affect the output of the Services or increase the risks in performing or receiving the Services; 3. will not adversely affect the interfaces or interoperability of the Services with any of the Authority’s IT infrastructure; and 4. will not require a change to this Contract; |
| “Operational Service Commencement Date” | in relation to an Operational Service, the later of:   1. the date identified in the Operational Services Implementation Plan upon which the Operational Service is to commence; and 2. where the Implementation Plan states that the Supplier must have Achieved the relevant ATP Milestone before it can commence the provision of that Operational Service, the date upon which the Supplier Achieves the relevant ATP Milestone; |
| “Operational Services” | the operational services described as such in the Services Description; |
| “Optional Services” | the services described as such in Schedule 2 (*Services Description*) which are to be provided by the Supplier if required by the Authority in accordance with Clause 5.10 (*Optional Services*); |
| “Optional Services Implementation Plan” | the implementation plan to effect the Optional Services agreed between the Parties prior to the Effective Date and, if not agreed prior to the Effective Date, to be developed by the Supplier and approved by the Authority; |
| “Other Supplier” | any supplier to the Authority (other than the Supplier) which is notified to the Supplier from time to time; |
| “Outline Implementation Plan” | the outline plan set out at Annex A of Schedule 9 (*Implementation Plan*); |
| “Parent Undertaking” | has the meaning set out in section 1162 of the Companies Act 2006; |
| “Partial Termination” | the partial termination of this Contract to the extent that it relates to the provision of any part of the Services as further provided for in Clause 31.2.2 (*Termination by the Authority*) or 31.3.2 (*Termination by the Supplier*) or otherwise by mutual agreement by the Parties; |
| “Parties” and “Party” | have the meanings respectively given on page 1 of this Contract; |
| “Performance Failure” | a KPI Failure or a PI Failure; |
| “Performance Indicators” | the Key Performance Indicators and the Subsidiary Performance Indicators; |
| “Permitted Maintenance” | has the meaning given in Clause 9.4 (*Maintenance*); |
| “Performance Monitoring Report” | has the meaning given in Schedule 3 (*Performance Levels*); |
| “Personal Data” | has the meaning given in the UK GDPR or the EU GDPR as the context requires; |
| “Personal Data Breach” | has the meaning given in the UK GDPR or the EU GDPR as the context requires; |
| “PI Failure” | a failure to meet the Target Performance Level in respect of a Subsidiary Performance Indicator; |
| “PI Service Threshold” | shall be as set out against the relevant Subsidiary Performance Indicator in Table 2 in Part A of Annex 1 of Schedule 3 (*Performance Levels*); |
| “Preceding Services” | has the meaning given in Clause 5.2.2(a) (*Standard of Services*); |
| “Prescribed Person” | a legal adviser, an MP, or an appropriate body which a whistle-blower may make a disclosure to as detailed in ‘Whistleblowing: list of prescribed people and bodies’, available online at: <https://www.gov.uk/government/publications/blowing-the-whistle-list-of-prescribed-people-and-bodies--2/whistleblowing-list-of-prescribed-people-and-bodies>[, as updated from time to time;](https://www.gov.uk/government/publications/blowing-thewhistle-list-of-prescribed-people-and-bodies--2/whistleblowing-listof-prescribed-people-and-bodies,%20as%20updated%20from%20time%20to%20time;) |
| "Processing" | has the meaning given to it in the UK GDPR or the EU GDPR as the context requires, and "Process" shall be construed accordingly; |
| “Processor” | has the meaning given to it under the UK GDPR or the EU GDPR as the context requires; |
| “Processor Personnel” | all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Sub-processor engaged in the performance of its obligations under this Contract; |
| “Programme Board” | the body described in Paragraph 5 of Schedule 17 (*Governance*); |
| “Protective Measures” | appropriate technical and organisational measures designed to ensure compliance with obligations of the Parties arising under Data Protection Legislation which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it, including those outlined in Schedule 5 (*Security Management*) and Schedule 26 *(Processing Personal Data)*; |
| “Project Specific IPRs” | 1. Intellectual Property Rights in items created by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Contract and updates and amendments of these items including (but not limited to) database schema; and/or 2. Intellectual Property Rights arising as a result of the performance of the Supplier’s obligations under this Contract;   but shall not include the Supplier Background IPRs or the Specially Written Software; |
| "Provisional Supplier Personnel List" | has the meaning given in Schedule 24 (*Staff Transfer*); |
| “Public Sector Dependent Supplier” | a supplier where that supplier, or that supplier’s group has Annual Revenue of £50 million or more of which over 50% is generated from UK Public Sector Business; |
| “Publishable Performance Information” | any of the information that the Authority is permitted or required to publish by the Procurement Act 2023, any Regulations published under it and any Procurement Policy Notes, relating to the performance of the Supplier against any Performance Indicator and any information contained in any Performance Monitoring Report; |
| “Quality Plans” | has the meaning given in Clause 6.1 (*Quality Plans*); |
| “Quarter” | the first three Service Periods and each subsequent three Service Periods (save that the final Quarter shall end on the date of termination or expiry of this Contract); |
| “Recipient” | has the meaning given in Clause 19.1 (*Confidentiality*); |
| “Recall” | a request by the Supplier to return Goods to the Supplier or the manufacturer after the discovery of safety issues or defects (including defects in the IPR rights) that might endanger health or hinder performance; |
| “Recipient” | has the meaning given in Clause 19.1 (*Confidentiality*); |
| “Records” | has the meaning given in Schedule 20 (*Reports and Records Provisions*); |
| “Rectification Plan” | a plan to address the impact of, and prevent the reoccurrence of, a Notifiable Default; |
| “Rectification Plan Failure” | 1. the Supplier failing to submit or resubmit a draft Rectification Plan to the Authority within the timescales specified in Clauses 25.4 (*Submission of the draft Rectification Plan*) or 25.8 (*Agreement of the Rectification Plan*); 2. the Authority, acting reasonably, rejecting a revised draft of the Rectification Plan submitted by the Supplier pursuant to Clause 25.7 (*Agreement of the Rectification Plan*); 3. the Supplier failing to rectify a material Default within the later of:    1. 30 Working Days of a notification made pursuant to Clause 25.2 (*Notification*); and    2. where the Parties have agreed a Rectification Plan in respect of that material Default and the Supplier can demonstrate that it is implementing the Rectification Plan in good faith, the date specified in the Rectification Plan by which the Supplier must rectify the material Default; 4. a Material KPI Failure re-occurring in respect of the same Key Performance Indicator for the same (or substantially the same) root cause in any of the 3 Measurement Periods subsequent to the Measurement Period in which the initial Material KPI Failure occurred; 5. the Supplier not Achieving a Key Milestone by the expiry of the Delay Deduction Period; and/or 6. following the successful implementation of a Rectification Plan, the same Notifiable Default recurring within a period of 6 months for the same (or substantially the same) root cause as that of the original Notifiable Default; |
| “Rectification Plan Process” | the process set out in Clauses 25.4 (*Submission of the draft Rectification Plan*) to 25.9 (*Agreement of the Rectification Plan*); |
| “Registers” | has the meaning given in Schedule 21 (*Exit Management*); |
| “Reimbursable Expenses” | has the meaning given in Schedule 11 (*Charges and Invoicing*); |
| “Relevant Authority” or “Relevant Authorities” | the Authority and the Cabinet Office Markets and Suppliers Team or, where the Supplier is a Strategic Supplier, the Cabinet Office Markets and Suppliers Team; |
| “Relevant IPRs” | IPRs used to provide the Services or as otherwise provided and/or licensed by the Supplier (or to which the Supplier has provided access) to the Authority or a third party in the fulfilment of the Supplier’s obligations under this Contract including IPRs in the Specially Written Software, the Supplier Non-COTS Software, the Supplier Non-COTS Background IPRs, the Third Party Non-COTS Software and the Third Party Non-COTS IPRs but excluding any IPRs in the Authority Software, the Authority Background IPRs, the Supplier COTS Software, the Supplier COTS Background IPRs, the Third Party COTS Software and/or the Third Party COTS IPRs; |
| “Relevant Preceding Services” | has the meaning given in Clause 5.2.2(b) (*Standard of Services*); |
| “Relevant Requirements” | all applicable Law relating to bribery, corruption and fraud, including the Bribery Act 2010 and any guidance issued by the Secretary of State for Justice pursuant to section 9 of the Bribery Act 2010; |
| “Relevant Transfer” | a transfer of employment to which the Employment Regulations applies; |
| “Relief Notice” | has the meaning given in Clause 29.2 (*Authority Cause*); |
| “Remedial Adviser” | the person appointed pursuant to Clause 27.2 (*Remedial Adviser*); |
| “Remedial Adviser Failure” | has the meaning given in Clause 27.6 (*Remedial Adviser*); |
| “Replacement Services” | any services which are the same as or substantially similar to any of the Services and which the Authority receives in substitution for any of the Services following the expiry or termination or Partial Termination of this Contract, whether those services are provided by the Authority internally and/or by any third party; |
| “Replacement Supplier” | any third party service provider of Replacement Services appointed by the Authority from time to time (or where the Authority is providing replacement Services for its own account, the Authority); |
| “Request For Information” | a Request for Information under the FOIA or the EIRs; |
| “Required Action” | has the meaning given in Clause 28.1.1 (*Step-In Rights*); |
| “Retained Deliverables” | has the meaning given in Clause 32.9.2 (*Payments by the Supplier*); |
| “Risk Register” | the register of risks and contingencies that have been factored into any Costs due under this Contract, a copy of which is set out in Annex 4 of Schedule 11 (*Charges and Invoicing*); |
| “Security Management Plan” | has the meaning given in Schedule 5 (*Security Management*); |
| "Security Requirements" | the security requirements set out in Appendix 1 to Schedule 5 (*Security Management*); |
| "Security Requirements for Development" | the security requirements for development set out in Appendix 2 to Schedule 5 (*Security Management*); |
| “Serious KPI Failure” | shall be as set out against the relevant Key Performance Indicator in Table 1 of Part A of Annex 1 of Schedule 3 (*Performance Levels*); |
| “Service Charges” | the periodic payments made in accordance with Schedule 11 (*Charges and Invoicing*) in respect of the supply of the Operational Services; |
| “Service Continuity Plan” | any plan prepared pursuant to Paragraph 2 of Schedule 22 (*Service Continuity Plan and Corporate Resolution Planning*) as may be amended from time to time; |
| “Service Continuity Services” | the business continuity, disaster recovery and insolvency continuity services set out in Schedule 22 (*Service Continuity Plan and Corporate Resolution Planning*) |
| “Service Credit Cap” | 1. in the period of 12 months from the first Operational Service Commencement Date to occur after the Effective Date, [x]% of the Estimated Initial Service Charges; and 2. during the remainder of the Term, [x]% of the Service Charges paid and/or due to be paid to the Supplier under this Contract in the period of 12 months immediately preceding the Service Period in respect of which Service Credits are accrued; |
| “Service Credits” | credits payable by the Supplier due to the occurrence of 1 or more KPI Failures, calculated in accordance with Paragraph 3 of Part C of Schedule 11 (*Charges and Invoicing*); |
| “Service Period” | a calendar month, save that:   1. the first service period shall begin on the first Operational Service Commencement Date and shall expire at the end of the calendar month in which the first Operational Service Commencement Date falls; and 2. the final service period shall commence on the first day of the calendar month in which the Term expires or terminates and shall end on the expiry or termination of the Term; |
| “Service Points” | in relation to a KPI Failure, the points that are set out against the relevant Key Performance Indicator in the fifth column of the table in Annex 1 of Schedule 3 (*Performance Levels*); |
| “Services” | any and all of the services to be provided by the Supplier under this Contract, including those set out in Schedule 2 (*Services Description*); |
| “Service Transfer Date” | has the meaning given in Schedule 24 (*Staff Transfer*); |
| “Services Description” | the services description set out in Schedule 2 (*Services Description*); |
| “Severe KPI Failure” | shall be as set out against the relevant Key Performance Indicator in Table 1 of Part A of Annex 1 of Schedule 3 (*Performance Levels*); |
| “Sites” | any premises (including the Authority Premises, the Supplier’s premises or third party premises):   1. from, to or at which:    1. the Services are (or are to be) provided; or    2. the Supplier manages, organises or otherwise directs the provision or the use of the Services; or 2. where:    1. any part of the Supplier System is situated; or    2. any physical interface with the Authority System takes place; |
| “SME” | an enterprise falling within the category of micro, small and medium-sized enterprises defined by the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises; |
| “Social Value” | the additional social benefits that can be achieved in the delivery of the Contract, set out in the Authority’s Requirements; |
| “Social Value PI” | the Social Value performance indicators set out in Table 2 of Part A of Annex 1 of Schedule 3 (*Performance Levels*); |
| “Social Value KPI” | the Social Value key performance indicators set out in Table 1 of Part A of Annex 1 of Schedule 3 (*Performance Levels*); |
| “Software” | Specially Written Software, Supplier Software and Third Party Software; |
| “Software Supporting Materials” | has the meaning given in Paragraph 1.1.1 of Schedule 27 (*Intellectual Property Rights*) (*Specially Written Software and Project Specific IPRs*); |
| “Source Code” | computer programs and/or data in eye-readable form and in such form that it can be compiled or interpreted into equivalent binary code together with all related design comments, flow charts, technical information and documentation necessary for the use, reproduction, maintenance, modification and enhancement of such software; |
| “Specially Written Software” | any software (including database software, linking instructions, test scripts, compilation instructions and test instructions) created by the Supplier (or by a Sub-contractor or other third party on behalf of the Supplier) specifically for the purposes of this Contract, including any modifications or enhancements to Supplier Software or Third Party Software created specifically for the purposes of this Contract. |
| “Specific Change in Law” | a Change in Law that relates specifically to the business of the Authority and which would not affect a Comparable Supply; |
| “Staffing Information” | has the meaning given in Schedule 24 (*Staff Transfer*); |
| “Standards” | the standards, polices and/or procedures identified in Schedule 4 (*Standards*); |
| “Step-In Notice” | has the meaning given in Clause 28.1 (*Step-In Rights*); |
| “Step-In Trigger Event” | 1. any event falling within the definition of a Supplier Termination Event; 2. a Default by the Supplier that is materially preventing or materially delaying the performance of the Services or any material part of the Services; 3. the Authority considers that the circumstances constitute an emergency despite the Supplier not being in breach of its obligations under this Contract; 4. the Authority being advised by a regulatory body that the exercise by the Authority of its rights under Clause 28 (*Step-In Rights*) is necessary; 5. the existence of a serious risk to the health or safety of persons, property or the environment in connection with the Services; and/or 6. a need by the Authority to take action to discharge a statutory duty; |
| “Step-Out Date” | has the meaning given in Clause 28.5.2 (*Step-In Rights*); |
| “Step-Out Notice” | has the meaning given in Clause 28.5 (*Step-In Rights*); |
| “Step-Out Plan” | has the meaning given in Clause 28.6 (*Step-In Rights*); |
| “Strategic Supplier” | those suppliers to government listed at <https://www.gov.uk/government/publications/strategic-suppliers>; |
| “Sub-contract” | any contract or agreement (or proposed contract or agreement) between the Supplier (or a Sub-contractor) and any third party whereby that third party agrees to provide to the Supplier (or the Sub-contractor) all or any part of the Services or facilities or services which are material for the provision of the Services or any part thereof or necessary for the management, direction or control of the Services or any part thereof; |
| “Sub-contractor” | any third party with whom:   1. the Supplier enters into a Sub-contract; or 2. a third party under (a) above enters into a Sub-contract,   or the servants or agents of that third party; |
| “Sub-processor” | any third party appointed to Process Personal Data on behalf of the Processor related to this Contract; |
| “Subsidiary Performance Indicator” | the performance indicators set out in Table 2 of Part A of Annex 1 of Schedule 3 (*Performance Levels*); |
| “Subsidiary Undertaking” | has the meaning set out in section 1162 of the Companies Act 2006; |
| “Successor Body” | has the meaning given in Clause 34.4 (*Assignment and Novation*); |
| “Supplier Background IPRs” | 1. Intellectual Property Rights owned by the Supplier before the Effective Date, for example those subsisting in the Supplier’s standard development tools, program components or standard code used in computer programming or in physical or electronic media containing the Supplier’s Know-How or generic business methodologies; and/or 2. Intellectual Property Rights created by the Supplier independently of this Contract,   which in each case is or will be used before or during the Term for designing, testing implementing or providing the Services but excluding Intellectual Property Rights owned by the Supplier subsisting in the Supplier Software; |
| “Supplier COTS Background IPRs” | any embodiments of Supplier Background IPRs that:   1. the Supplier makes generally available commercially prior to the date of this Contract (whether by way of sale, lease or licence) on standard terms which are not typically negotiated by the Supplier save as to price; and 2. has a Non-trivial Customer Base; |
| “Supplier COTS Software” | Supplier Software (including open source software) that:   1. the Supplier makes generally available commercially prior to the date of this Contract (whether by way of sale, lease or licence) on standard terms which are not typically negotiated by the Supplier save as to price; and 2. has a Non-trivial Customer Base; |
| “Supplier Equipment” | the hardware, computer and telecoms devices and equipment used by the Supplier or its Sub-contractors (but not hired, leased or loaned from the Authority) for the provision of the Services; |
| “Supplier Group” | the Supplier, its Dependent Parent Undertakings and all Subsidiary Undertakings and Associates of such Dependent Parent Undertakings; |
| “Supplier Non-COTS Background IPRs” | any embodiments of Supplier Background IPRs that have been delivered by the Supplier to the Authority and that are not Supplier COTS Background IPRs; |
| “Supplier Non-COTS Software” | Supplier Software that is not Supplier COTS Software; |
| “Supplier Non‑Performance” | has the meaning given in Clause 29.1 (*Authority Cause*); |
| “Supplier Personnel” | any individual engaged, directly or indirectly, or employed by the Supplier or any Sub-contractor, in the management or performance of the Supplier's obligations under this Contract; |
| “Supplier Profit” | has the meaning given in Schedule 11 (*Charges and Invoicing*); |
| “Supplier Profit Margin” | has the meaning given in Schedule 11 (*Charges and Invoicing*); |
| “Supplier Representative” | the representative appointed by the Supplier pursuant to Clause 11.3 (*Representatives*); |
| “Supplier Software” | software which is proprietary to the Supplier (or an Affiliate of the Supplier) and which is or will be used by the Supplier for the purposes of providing the Services, including the software specified as such in section 8 *(Software)* of the Front Sheet; |
| “Supplier Solution” | the Supplier’s solution for the Services set out in Schedule 8 (*Supplier Solution*) including any Annexes of that Schedule; |
| “Supplier System” | the information and communications technology system used by the Supplier in implementing and performing the Services including the Software, the Supplier Equipment, configuration and management utilities, calibration and testing tools and related cabling (but excluding the Authority System); |
| “Supplier Termination Event” | 1. the Supplier’s level of performance constituting a Critical Performance Failure in accordance with Clause 7.6; 2. the Supplier committing a material Default which is irremediable; 3. as a result of the Supplier’s Default, the Authority incurring Losses in any Contract Year which exceed 80% of the value of the aggregate annual liability cap for that Contract Year as set out in Clause 23.4.4 (*Financial and other Limits*); 4. a Remedial Adviser Failure; 5. a Rectification Plan Failure; 6. where a right of termination is expressly reserved in this Contract, including pursuant to:    1. Clause 15 *(Supply Chain Protection)*;    2. Clause 17 (*IPRs Indemnity*);    3. Clause 33 (*Compliance*)    4. Clause 37.4 *(Exclusions)*;    5. Paragraph 6 of Schedule 14 (*Financial Distress*); and/or    6. Paragraph 3 of Part B to Schedule 22 (*Service Continuity Plan and Corporate Resolution Planning*); 7. the representation and warranty given by the Supplier pursuant to Clause 3.2.8 (*Warranties*) being materially untrue or misleading; 8. the Supplier committing a material Default under any of the following Clauses:    1. Clause 5.5.10 (*Services*);    2. Clause 21 (*Protection of Personal Data*);    3. Clause 20 (*Transparency and Freedom of Information*);    4. Clause 19 (*Confidentiality*);    5. Clause 33 (*Compliance*);    6. in respect of any Security Requirements or Cyber Essentials obligations set out in Schedule 2 (*Services Description*) or Schedule 5 (*Security Management*);    7. in respect of any requirements set out in Schedule 27 *(Intellectual Property Rights)*; and/or    8. in respect of any requirements set out in Schedule 24 (*Staff Transfer*); 9. any failure by the Supplier to implement the changes set out in a Benchmark Report as referred to in Paragraph 5.9 of Schedule 13 (*Benchmarking*); 10. an Insolvency Event occurring in respect of the Supplier or the Guarantor; 11. the Guarantee ceasing to be valid or enforceable for any reason (without the Guarantee being replaced with a comparable guarantee to the satisfaction of the Authority with the Guarantor or with another guarantor which is acceptable to the Authority); 12. a change of Control of the Supplier or a Guarantor unless:     1. the Authority has given its prior written consent to the particular change of Control, which subsequently takes place as proposed; or     2. the Authority has not served its notice of objection within 6 months of the later of the date on which the change of Control took place or the date on which the Authority was given notice of the change of Control; 13. a change of Control of a Key Sub-contractor unless, within 6 months of being notified by the Authority that it objects to such change of Control, the Supplier terminates the relevant Key Sub-contract and replaces it with a comparable Key Sub-contract which is approved by the Authority pursuant to Clause 15.6 (*Appointment of Key Sub-contractors*); 14. the Supplier committing a material Default under Paragraphs 7.1.1 or 7.1.2 of Part D of Schedule 24 (*Staff Transfer*); 15. a failure by the Supplier to comply in the performance of the Services with legal obligations in the fields of environmental, social or labour law; 16. in relation to Schedule 5 (*Security Management*):     1. the Authority has issued two rejection notices in respect of the Security Management Plan;     2. the Supplier fails to implement a change required by the Required Changes Register in accordance with the timescales set out in the Required Changes Register;     3. Supplier COTS Software and Third Party COTS Software is not within mainstream support unless the Authority has agreed in writing;     4. the Supplier fails to patch vulnerabilities in accordance with the Security Requirements set out in the Appendices to Schedule 5 (*Security Management*)*;* and/or,     5. the Supplier fails to comply with the Incident Management Process; 17. the Supplier is in material Default of any Joint Controller Agreement relating to the Contract; 18. a Default that occurs and continues to occur on one or more occasions within 6 Months following the Authority serving a warning notice on the Supplier that it may terminate for persistent breach of the Contract; or 19. the Supplier or its Affiliates embarrass or bring the Authority into disrepute or diminish the public trust in them; |
| "Supply Chain Intermediary" | any entity (including any company or partnership) in an arrangement with a Worker, where the Worker performs or is under an obligation personally to perform, services for the Authority; |
| [Optional: “Supply Chain Map”  *[Guidance: Include this definition if Optional Clause 33.8.15 is included in the Core Terms]* | details of (i) the Supplier, (ii) all Sub-contractors and (iii) any other entity that the Supplier is aware is in its supply chain that is not a Subcontractor, setting out at least:   1. the name, registered office and company registration number of each entity in the supply chain; 2. the function of each entity in the supply chain; and   the location of any premises at which an entity in the supply chain carries out a function in the supply chain;] |
| “Target Performance Level” | the minimum level of performance for a Performance Indicator which is required by the Authority, as set out against the relevant Performance Indicator in the tables in Annex 1 of Schedule 3 (*Performance Levels*); |
| “Term” | the period commencing on the Effective Date and ending on the expiry of the Initial Term or any Extension Period or on earlier termination of this Contract; |
| “Termination Assistance Notice” | has the meaning given in Paragraph 5 of Schedule 21 (*Exit Management*); |
| “Termination Assistance Period” | in relation to a Termination Assistance Notice, the period specified in the Termination Assistance Notice for which the Supplier is required to provide the Termination Services as such period may be extended pursuant to Paragraph 5.2 of Schedule 21 (*Exit Management*); |
| “Termination Date” | the date set out in a Termination Notice on which this Contract (or a part of it as the case may be) is to terminate; |
| “Termination Notice” | a written notice of termination given by one Party to the other, notifying the Party receiving the notice of the intention of the Party giving the notice to terminate this Contract (or any part thereof) on a specified date and setting out the grounds for termination; |
| “Termination Payment” | the payment determined in accordance with Schedule 12 (*Payments on Termination*); |
| “Termination Services” | the services and activities to be performed by the Supplier pursuant to the Exit Plan, including those activities listed in Annex 1 of Schedule 21 (*Exit Management*), and any other services required pursuant to the Termination Assistance Notice; |
| “Test Issues” | has the meaning given in Schedule 10 (*Testing Procedures*); |
| “Tests” and “Testing” | any tests required to be carried out under this Contract, as further described in Schedule 10 (*Testing Procedures*) and “Tested” shall be construed accordingly; |
| “Test Success Criteria” | has the meaning given in Schedule 10 (*Testing Procedures*); |
| “Third Party Auditor” | an independent third party auditor as appointed by the Authority from time to time to confirm the completeness and accuracy of information uploaded to the Virtual Library in accordance with the requirements outlined in Schedule 20 (*Reports and Records Provisions*); |
| “Third Party Beneficiary” | has the meaning given in Clause 41.1 (*Third Party Rights*); |
| "Third Party Contract" | a contract with a third party entered into by the Supplier exclusively for the purpose of delivering the Services, as listed in section 7 *(Third Party Contracts)* of the Front Sheet; |
| “Third Party COTS IPRs” | Third Party IPRs that:   1. the Supplier makes generally available commercially prior to the date of this Contract (whether by way of sale, lease or licence) on standard terms which are not typically negotiated by the Supplier save as to price; and 2. has a Non-trivial Customer Base; |
| “Third Party COTS Software” | Third Party Software (including open source software) that:   1. the supplier makes generally available commercially prior to the date of this Contract (whether by way of sale, lease or licence) on standard terms which are not typically negotiated by the supplier save as to price; and 2. has a Non-trivial Customer base; |
| “Third Party IPRs” | Intellectual Property Rights owned by a third party, but excluding Intellectual Property Rights owned by the third party subsisting in any Third Party Software, which in any case is, will be or is proposed to be used by the Supplier for the purposes of providing the Services; |
| “Third Party Non-COTS IPRs” | Third Party IPRs that are not Third Party COTS IPRs; |
| “Third Party Non-COTS Software” | Third Party Software that is not Third Party COTS Software; |
| “Third Party Provisions” | has the meaning given in Clause 41.1 (*Third Party Rights*); |
| “Third Party Software” | Software which is proprietary to any third party (other than an Affiliate of the Supplier) or any Open Source Software which in any case is, will be or is proposed to be used by the Supplier for the purposes of providing the Services, including the software specified as such in section 8 *(Software)* of the Front Sheet; |
| “Transferring Assets” | has the meaning given in Paragraph 6.2.1 of Schedule 21 (*Exit Management*); |
| “Transferring Authority Employees” | has the meaning given in Schedule 24 (*Staff Transfer*); |
| “Transferring Former Supplier Employees” | has the meaning given in Schedule 24 (*Staff Transfer*); |
| “Transferring Supplier Employees” | has the meaning given in Schedule 24 (*Staff Transfer*); |
| “Transparency Information” | (a) any information or notices, permitted or required to be published by the Procurement Act 2023, any Regulations published under it, and any PPNs, subject to any exemptions set out in sections 94 and 99 of the Procurement Act 2023, which shall be determined by the Authority taking into account Commercially Sensitive Information as set out in the Front Sheet;  (b) any information about this Contract, including the content of this Contract requested and required to be disclosed under FOIA or the EIRs and any changes to this Contract agreed from time to time, subject to any exemptions, which shall be determined by the Authority taking into account Commercially Sensitive Information as set out in the Front Sheet;  (c) the Publishable Performance Information, subject to any exemptions set out in sections 94 and 99 of the Procurement Act 2023, or under the provisions of FOIA, which shall be determined by the Authority taking into account Commercially Sensitive Information as set out in the Front Sheet; and  (d) any information which is published in accordance with guidance issued by His Majesty's Government, from time to time; |
| “UK” | the United Kingdom; |
| “UK GDPR” | has the meaning as set out in Section 3(10) of the DPA 2018, supplemented by Section 205(4) of the DPA 2018; |
| “UK Public Sector Business” | any goods, service or works provision to UK public sector bodies, including Central Government Departments and their arm’s length bodies and agencies, non-departmental public bodies, NHS bodies, local authorities, health bodies, police, fire and rescue, education bodies and devolved administrations; |
| “Unacceptable KPI Failure” | the Supplier failing to achieve the KPI Service Threshold in respect of more than 50% of the Key Performance Indicators that are measured in that Service Period; |
| “Unconnected Sub‑contract” | any contract or agreement which is not a Sub-contract and is between the Supplier and a third party (which is not an Affiliate of the Supplier) and is a qualifying contract under regulation 6 of The Reporting on Payment Practices and Performance Regulations 2017; |
| “Unconnected Sub‑contractor” | any third party with whom the Supplier enters into an Unconnected Sub-contract; |
| “Unrecovered Payment” | has the meaning given in Schedule 12 (*Payments on Termination*); |
| “Updates” | in relation to any Software and/or any Deliverable means a version of such item which has been produced primarily to overcome Defects in, or to improve the operation of, that item; |
| “Update Requirement” | the occurrence of an event detailed in Schedule 20 (*Reports and Records Provisions*) (Annex 2: *Records To Upload To Virtual Library*) which requires the Supplier to update the relevant information hosted on the Virtual Library; |
| “Upgrades” | any patch, New Release or upgrade of Software and/or a Deliverable, including standard upgrades, product enhancements, and any modifications, but excluding any Update which the Supplier or a third party software supplier (or any Affiliate of the Supplier or any third party) releases during the Term; |
| "US Data Privacy Framework" | as applicable: (a) the UK Extension to the EU-US Data Privacy Framework; and/or (b) the EU-US Data Privacy Framework; |
| “Valid” | in respect of an Assurance, has the meaning given to it in Paragraph 2.7 of Part B to Schedule 22 (*Service Continuity Plan and Corporate Resolution Planning*); |
| “VAT” | value added tax as provided for in the Value Added Tax Act 1994; |
| “VCSE” | a non-governmental organisation that is value-driven and which principally reinvests its surpluses to further social, environmental or cultural objectives; |
| “Virtual Library” | the data repository hosted by the Supplier containing the information about this Contract and the Services provided under it in accordance with Schedule 20 (*Reports and Records Provisions*); |
| "Worker" | any individual that personally performs, or is under an obligation personally to perform services for the Authority; and |
| “Working Day” | any day other than a Saturday, Sunday or public holiday in England and Wales. |

Schedule 2

Services Description

# Schedule 2: Services Description

1. Definitions
   1. In this Schedule, the following definitions shall apply:

**[Insert** definitions as required]

1. Introduction
   1. [**Outline** why the Authority has identified that it needs the Supplier to provide the Services.]
   2. This Schedule sets out the intended scope of the Services to be provided by the Supplier and to provide a description of what each Service entails.
2. Services Description
   1. Contract Modifications: *[Guidance: Please note that if the Authority intends to rely on the permitted modification ground contained in Paragraph 1 (Provided for in the contract) of Schedule 8 to the Procurement Act, the Authority must include details of the possibility of modification unambiguously within the tender notice or the transparency notice and within the final version of the Contract but the modification must not change the overall nature of the Contract. It is important to include as much information as possible to ensure that this ground can be relied upon. If the Authority intends to rely on the permitted modification ground contained in Paragraph 5 (Materialisation of a known risk) of Schedule 8 to the Procurement Act, the Authority must include details of the known risk that could jeopardise the satisfactory performance of the Contract but which cannot be addressed from the outset within the tender notice or the transparency notice, in as much detail as possible, prior to awarding the contract.]*
   2. Implementation Services – [**Description** of the services to be provided by the Supplier for the design, build, test, implementation and roll out of the Operational Services]
   3. Operational Services – [**Description** of the business as usual services including Operational Hours]
   4. Interface Requirements - **[Insert** as required
      1. technical interface and
      2. management obligations/responsibilities]
   5. Security Requirements **[Insert** as required]
   6. **Social Value Requirements** – [**Description** of the additional social, environmental and economic benefits to be delivered in line with the [**Public Services (Social Value) Act 2012**](https://www.gov.uk/government/publications/social-value-act-information-and-resources/social-value-act-information-and-resources), PPN 002 - taking account of social value in the award of central government contracts, and Authority policies and practices]
   7. Other Authority Requirements – [Description of any other requirements of the Authority e.g. wider sustainability requirements and other Authority commitments]
   8. Optional Services - **[Insert** as required]

Schedule 3

Performance Levels

# Schedule 3: Performance Levels

1. Definitions
   1. In this Schedule, the following definitions shall apply:

|  |  |
| --- | --- |
| **“Available”** | has the meaning given in Paragraph 1.1 of Part B of Annex 1; |
| **“End User”** | any person authorised by the Authority to use the IT Environment and/or the Services; |
| **“Help Desk”** | the single point of contact help desk set up and operated by the Supplier for the purposes of this Contract; |
| **“Non-Available”** | in relation to the IT Environment or the Services, that the IT Environment or the Services are not Available; |
| **“Performance Monitoring Report”** | has the meaning given in Paragraph 1.1.1 of Part B; |
| **“Performance Review Meeting”** | the regular meetings between the Supplier and the Authority to manage and review the Supplier’s performance under this Contract, as further described in Paragraph 1.5 of Part B; |
| **“Repeat KPI Failure”** | has the meaning given in Paragraph 3.1 of Part A; |
| **“Satisfaction Survey”** | has the meaning given in Paragraph 6.1 of Part B of Annex 1; |
| **“Service Availability”** | has the meaning given in Paragraph 2 of Part B of Annex 1; |
| **“Service Downtime”** | any period of time during which any of the Services are not Available; and |
| **“System Response Time”** | has the meaning given in Paragraph 3.1 of Part B of Annex 1. |

## Part A: Performance Indicators and Service Credits

1. Performance Indicators
   1. Annex 1 sets out the Key Performance Indicators and Subsidiary Performance Indicators which the Parties have agreed shall be used to measure the performance of the Services and Social Value by the Supplier.
   2. The Supplier shall monitor its performance against each Performance Indicator and shall send the Authority a report detailing the level of service actually achieved in accordance with Part B B to enable the Authority to assess the Supplier’s performance against each Key Performance Indicators and Subsidiary Performance Indicator in each Measurement Period.
   3. Service Points, and therefore Service Credits, shall accrue for any KPI Failure and shall be calculated in accordance with Paragraphs 2, 3 and 5.
2. Service Points
   1. If the level of performance of the Supplier during a Service Period achieves the Target Performance Level in respect of a Key Performance Indicator, no Service Points shall accrue to the Supplier in respect of that Key Performance Indicator.
   2. If the level of performance of the Supplier during a Service Period is below the Target Performance Level in respect of a Key Performance Indicator, Service Points shall accrue to the Supplier in respect of that Key Performance Indicator as set out in Paragraph 2.3.
   3. The number of Service Points that shall accrue to the Supplier in respect of a KPI Failure shall be the applicable number as set out in Annex 1 depending on whether the KPI Failure is a Minor KPI Failure, a Serious KPI Failure or a Severe KPI Failure, unless the KPI Failure is a Repeat KPI Failure when the provisions of Paragraph 3.2 shall apply.
3. Repeat KPI Failures and Related KPI Failures

**Repeat** **KPI** **Failures**

* 1. If a KPI Failure occurs in respect of the same Key Performance Indicator in any two consecutive Measurement Periods, the second and any subsequent such KPI Failure shall be a “**Repeat KPI Failure**”.
  2. The number of Service Points that shall accrue to the Supplier in respect of a KPI Failure that is a Repeat KPI Failure shall be calculated as follows:

**SP = P x** **2**

where:

**SP =** the number of Service Points that shall accrue for the Repeat KPI Failure; and

**P =** the applicable number of Service Points for that KPI Failure as set out in Annex 1 depending on whether the Repeat KPI Failure is a Minor KPI Failure, a Serious KPI Failure, a Severe KPI Failure or a failure to meet the KPI Service Threshold.

**[Optional: Worked example based on the following Service Points regime for Service Availability:**

| Service Availability Severity Levels | Service Points |
| --- | --- |
| Target Performance Level: 99% | 0 |
| Minor KPI Failure: 98.0% - 98.9% | 1 |
| Serious KPI Failure: 97.0% - 97.9% | 2 |
| Severe KPI Failure: 96.0% - 96.9% | 3 |
| KPI Service Threshold: below 96% | 4 |

**Example 1:**

If the Supplier achieves Service Availability of 98.5% in a given Measurement Period, it will incur a Minor KPI Failure for Service Availability in that Measurement Period and accordingly accrue 1 Service Point. If, in the next Measurement Period, it achieves Service Availability of 96.5%, it will incur a Severe KPI Failure and accordingly accrue 3 Service Points, but as the failure is a Repeat Failure, this amount is doubled and so the Supplier will incur 6 Service Points for the failure (i.e. SP = 3 x 2). If in the next Measurement Period it achieves Service Availability of 96.5%, the Supplier will again incur 6 Service Points.

**Example 2:**

If the Supplier achieves Service Availability of 96.5% in a given Measurement Period, it will incur a Severe KPI Failure for Service Availability in that Measurement Period and accordingly accrue 3 Service Points. If, in the next Measurement Period, it achieves Service Availability of 98.5%, it will incur a Minor KPI Failure and accordingly accrue 1 Service Point, but as the failure is a Repeat Failure, this amount is doubled and so the Supplier will incur 2 Service Points for the failure (i.e. SP = 1 x 2). If in the next Measurement Period it achieves Service Availability of 96.5%, the Supplier will incur 6 Service Points.]

**Related KPI Failures**

* 1. If any specific Key Performance Indicators refer to both Service Availability and System Response Times, the System Response Times achieved by the Supplier for any period of time during a Service Period during which the relevant Service or element of a Service is determined to be Non-Available shall not be taken into account in calculating the average System Response Times over the course of that Service Period. Accordingly, the Supplier shall not incur any Service Points for failure to meet System Response Times in circumstances where such failure is a result of, and the Supplier has already incurred Service Points for, the Service being Non-Available.

1. Permitted Maintenance
   1. The Supplier shall be allowed to book a maximum of **[insert** number] hours Service Downtime for Permitted Maintenance in any one Service Period which shall take place between the hours and on the day specified in the Maintenance Schedule unless otherwise agreed in writing with the Authority.
2. Service Credits

* 1. Schedule 11 (*Charges and Invoicing*) sets out the mechanism by which Service Points shall be converted into Service Credits.
  2. The Authority shall use the Performance Monitoring Reports provided pursuant to Part B, among other things, to verify the calculation and accuracy of the Service Credits (if any) applicable to each Service Period.

## Part B: Performance Monitoring

1. Performance Monitoring and Performance Review
   1. Within 10 Working Days of the end of each Service Period, the Supplier shall provide:
      1. a report to the Authority Representative which summarises the performance by the Supplier against each of the Performance Indicators as more particularly described in Paragraph 1.2 (the “**Performance Monitoring Report**”); and
      2. a report created by the Supplier to the Authority’s senior responsible officer which summarises the Supplier’s performance over the relevant Service Period as more particularly described in Paragraph 1.3 (the “**Balanced Sustainability Report**”).

**Performance Monitoring** **Report**

* 1. The Performance Monitoring Report shall be in such format as agreed between the Parties from time to time and contain, as a minimum, the following information:

**Information in respect of the Service Period just** **ended**

* + 1. for each Key Performance Indicator and Subsidiary Performance Indicator, the actual performance achieved over the Service Period and, where a Measurement Period has ended in the period covered by the Performance Monitoring Report, the most recently ended Measurement Period;
    2. a summary of all Performance Failures that occurred during the Service Period;
    3. the severity level of each KPI Failure which occurred during the Service Period and, where a Measurement Period has ended in the period covered by the Performance Monitoring Report, the most recently ended Measurement Period and whether each PI Failure which occurred during the Service Period and Measurement Period (if applicable) fell below the PI Service Threshold;
    4. which Performance Failures remain outstanding and progress in resolving them;
    5. for any Material KPI Failures or Material PI Failures occurring during the Service Period, the cause of the relevant KPI Failure or PI Failure and the action being taken to reduce the likelihood of recurrence;
    6. the status of any outstanding Rectification Plan processes, including:
       1. whether or not a Rectification Plan has been agreed; and
       2. where a Rectification Plan has been agreed, a summary of the Supplier’s progress in implementing that Rectification Plan;
    7. for any Repeat Failures, actions taken to resolve the underlying cause and prevent recurrence;
    8. the number of Service Points awarded in respect of each KPI Failure;
    9. the Service Credits to be applied, indicating the KPI Failure(s) to which the Service Credits relate;
    10. the conduct and performance of any agreed periodic tests that have occurred, such as the annual failover test of the Service Continuity Plan;
    11. relevant particulars of any aspects of the Supplier’s performance which fail to meet the requirements of this Contract;
    12. such other details as the Authority may reasonably require from time to time; and

**Information in respect** of **previous Service** **Periods**

* + 1. a rolling total of the number of Performance Failures that have occurred over the past six Service Periods;
    2. the amount of Service Credits that have been incurred by the Supplier over the past six Service Periods;
    3. the conduct and performance of any agreed periodic tests that have occurred in such Service Period such as the annual failover test of the Service Continuity Plan; and

**Information in respect of the next** **Quarter**

* + 1. any scheduled Service Downtime for Permitted Maintenance and Updates that has been agreed between the Authority and the Supplier for the next Quarter.

**Balanced Sustainability** **Report**

* 1. The Balanced Sustainability Report shall be presented in the form of an online accessible dashboard and, as a minimum, shall contain a high level summary of the Supplier’s performance over the relevant Service Period, including details of the following:
     1. financial indicators;
     2. the Target Performance Levels achieved;
     3. behavioural indicators;
     4. performance against its obligation to pay its Sub-contractors within thirty (30) days of receipt of an undisputed invoice;
     5. performance against its obligation to pay its Unconnected Sub-contractors within sixty (60) days of receipt of an invoice;
     6. Milestone trend chart, showing performance of the overall programme;
     7. sustainability indicators, for example net zero carbon, waste minimisation or performance to support a circular economy; and
     8. Social Value (as applicable).
  2. The Performance Monitoring Report and the Balanced Sustainability Report shall be reviewed and their contents agreed by the Parties at the next Performance Review Meeting held in accordance with Paragraph 1.5.
  3. The Parties shall attend meetings on a monthly basis (unless otherwise agreed) to review the Performance Monitoring Reports and the Balanced Sustainability Reports. The Performance Review Meetings shall (unless otherwise agreed):
     1. take place within 5 Working Days of the Performance Monitoring Report being issued by the Supplier;
     2. take place at such location and time (within normal business hours) as the Authority shall reasonably require (unless otherwise agreed in advance); and
     3. be attended by the Supplier Representative and the Authority Representative.
  4. The Authority shall be entitled to raise any additional questions and/or request any further information from the Supplier regarding any KPI Failure and/or PI Failure.
  5. The table in Paragraph 5 of Part A of Annex 1 describes how the severity levels set out under each of the Performance Indicators will be mapped to the performance ratings prescribed under Regulation 38(5) of the Procurement Regulations 2024. The mapping set out in that table will be applied by the Authority when publishing relevant Transparency Information relating to the Performance Indicators and/or the Supplier's performance against the relevant Performance Indicators pursuant to Section 52(3) and/or Section 71(2) of the Procurement Act 2023 and the associated Regulations.
  6. The Supplier acknowledges and agrees that, each time the Authority conducts an assessment of the Supplier's performance against a Performance Indicator, the Authority may publish information as required by Law in relation to that assessment.

1. Performance Records
   1. The Supplier shall keep appropriate documents and records (including Help Desk records, staff records, timesheets, training programmes, staff training records, goods received documentation, supplier accreditation records, complaints received etc) in relation to the Services being delivered. Without prejudice to the generality of the foregoing, the Supplier shall maintain accurate records of call histories for a minimum of 12 months and provide prompt access to such records to the Authority upon the Authority’s request. The records and documents of the Supplier shall be available for inspection by the Authority and/or its nominee at any time and the Authority and/or its nominee may make copies of any such records and documents.
   2. In addition to the requirement in Paragraph 2.1 to maintain appropriate documents and records, the Supplier shall provide to the Authority such supporting documentation as the Authority may reasonably require in order to verify the level of the performance of the Supplier both before and after each Operational Service Commencement Date and the calculations of the amount of Service Credits for any specified period.
   3. The Supplier shall ensure that the Performance Monitoring Report, the Balanced Sustainability Report (as well as historic Performance Monitoring Reports and historic Balance Scorecard Reports) and any variations or amendments thereto, any reports and summaries produced in accordance with this Schedule and any other document or record reasonably required by the Authority are available to the Authority on-line and are capable of being printed.
2. Performance Verification
   1. The Authority reserves the right to verify the Availability of the IT Environment and/or the Services and the Supplier’s performance under this Contract against the Performance Indicators including by sending test transactions through the IT Environment or otherwise.

## Annex 1: Key Performance Indicators and Subsidiary Performance Indicators

## Part A: Key Performance Indicators and Subsidiary Performance Indicators Tables

***[Guidance: The tables and calculations below are included by way of example only.***

***Key Performance Indicators (“KPIs”) and the Procurement Act 2023***

***The Procurement Act 2023 and the Procurement Regulations 2024 set out important provisions for contracts with an estimated value of more than £5 million as follows:***

* ***Section 52(1) of the Procurement Act 2023 requires an Authority to set at least 3 KPIs unless it considers that KPIs will not appropriately assess a supplier’s performance.***
* ***Section 52(3) of the Procurement Act 2023 requires Authorities to publish all of the KPIs set under section 52(1). In most cases, Authorities will satisfy this by complying with the obligation in section 53(3) of the of the Procurement Act 2023 which says they must publish a copy of any contract with an estimated value of more than £5 million.***
* ***In respect of contract details notices under the Procurement Regulations 2024:***
  + ***Regulation 32(2)(r) and regulation 35(2)(a) provides that an Authority must include a description of the 3 KPIs the Authority regards, at the time the contract details notice is published, as most material to performance of the contract obligations.***
  + ***Regulation 32(2)(s) and regulation 35(2)(a) instructs Authorities who have deemed KPIs not appropriate for assessing the performance of their contract, to explain why. Section 71(2) of the Procurement Act 2023 requires an Authority to assess and publish performance against the KPIs at least once in every period of twelve months throughout the life of the contract, and on termination of the contract.***
* ***In respect of contract performance notices under the Procurement Regulations 2024:***
  + ***Regulation 39(4)(d) and (e) provide that an Authority must include a description of the 3 KPIs that it regards as most material to performance of the contract obligations at the time the contract performance notice is published and a statement that the notice is being used to set out the Authority’s assessment of performance against those 3 KPIs.***
* ***It is worth noting that a Social Value KPI may be one included as one of these 3 KPIs reported in the contract detail notice, and contract performance notices, should an Authority regard it as most material to performance of the contract at the time.***

***It is possible that the KPIs selected as the top 3 may change throughout the life of the contract, meaning that those appearing in future contract performance notices may be different to those published at the time of contract award and within the contract details notice.***

***Authorities should note the exemptions in sections 94 and 99 of the Procurement Act 2023. If an Authority withholds information under section 94 of the Procurement Act 2023, it must publish the fact that the information is being withheld and which sub-section of section 94 it is being withheld under.***

***These obligations (and applicable exemptions) on publishing KPIs have been incorporated into the defined term of “Transparency Information” within this contract, and it is expected that performance against any KPIs set under the contract can be published. Authorities should refer to the KPI guidance published on Gov.uk (***[***https://www.gov.uk/government/publications/procurement-act-2023-guidance-documents-manage-phase/guidance-key-performance-indicators-html***](https://www.gov.uk/government/publications/procurement-act-2023-guidance-documents-manage-phase/guidance-key-performance-indicators-html)***) for further information.***

***Commercial Playbooks and KPIs***

***The Procurement Act 2023 expands the current KPI reporting requirement policy for Central Government Authorities and associated Arm's Length Bodies ("ALBs"). The requirements in the Procurement Act are in addition to (and so do not replace) those set out in the Commercial Playbooks. Please refer to the extra notes below the example table.***

***For example, where an Authority is a Central Government Department or ALB, they must:***

* ***in line with the*** [***Sourcing Playbook***](https://www.gov.uk/government/publications/the-sourcing-and-consultancy-playbooks)***, publish the top 3 operational KPIs for the Government’s most important contracts on a quarterly basis; and***
* ***where the Digital, Data and Technology Playbook (DDAT)*** [***(https://www.gov.uk/government/publications/the-digital-data-and-technology-playbook***](file:///C:/Users/Kate.Macey/Downloads/(https:/www.gov.uk/government/publications/the-digital-data-and-technology-playbook)***) applies to the Contract, comply with the DDAT policy requirements to publish 4 mandatory DDAT KPIs on a regular basis.***

***Social Value KPIs***

***In line with PPN 002 – Taking account of social value in the award of central government contracts, organisations (Central Government Departments & their ALBs) procurement-specific Social Value KPIs (“Social Value KPIs”) and formulae should be introduced that reflect the particular requirements of the procurement. All Social Value KPIs should be established using the Model Award Criteria and Reporting Metrics set out in the procurement documentation and in the tenderer’s proposals.***

***For Social Value KPIs, where the successful bidder proposes specific commitments in its tender proposal which are in addition to those set out in the procurement, then such commitments will also be used to establish Social Value KPIs.***

***Adjustments to the table and calculation approach below can be made as necessary.***

***The Authority should discuss Social Value with participants during pre-market engagement to inform the selection of relevant, proportionate and non-discriminatory questions and criteria from the Social Value Model, and to consider whether the market in question has a mature Social Value offering. Such Social Value KPIs will always comprise a combination of a deliverable and a numeric element, being specific, measurable and time-bound commitments, by which performance of that deliverable is to be measured***

***In the table below, Social Value KPIs may have an appropriate Service Credit level above 0% (zero percent) for markets which have a mature Social Value offering, where proportionate. When determining what are such appropriate levels, the Authority should consider what is proportionate in the context of the subject matter of the contract and its value, what is feasible in the circumstances, whether they provide sufficient incentive without driving up cost. The Authority should also consider whether Social Value goals are better served in each instance by tying Service Credits to the input cost of meeting the Social Value KPI or to the output benefit which meeting the Social Value KPI is expected to bring.***

***For less mature markets, the Authority may consider setting the Service Credit level for Social Value KPIs at 0% (zero percent), as the Rectification Plan Process will be a more appropriate remedy in these circumstances than Service Credits***.

***The Authority should ensure that the social value priorities to be delivered and how the Supplier will deliver these priorities are included in this Contract (for example in Schedule 2 (Services Description), Schedule 8 (Supplier Solution), and Schedule 9 (Implementation Plan)]***

The Key Performance Indicators and Subsidiary Performance Indicators that shall apply to the Operational Services and the Key Performance Indicators or Subsidiary Performance Indicators relating to Social Value are set out below:

### Key Performance Indicators

***[Guidance: Where a contracting authority is a Central Government Departments or one of their Arms-Length Bodies (ALBs):***

* ***in line with the*** [***Sourcing Playbook***](https://www.gov.uk/government/publications/the-sourcing-and-consultancy-playbooks)***, it is HMG’s intention to publish the top three (3) operational KPIs for the Government’s most important contracts on a quarterly basis; and***
* ***where the Digital, Data and Technology Playbook (DDAT) applies to the Contract, Central Government Departments and/or their ALBs must comply with the DDAT policy requirements to publish four (4) mandatory DDAT KPIs on a regular basis.]***

| No. | Key Performance Indicator Title | Definition | Measurement Period | Severity Levels | Service Points |
| --- | --- | --- | --- | --- | --- |
| KPI1 | [Service Availability] | See Paragraph 1 of Part B of this Annex |  | Target Performance Level: [99%]  Minor KPI Failure: [98.0% - 98.9%]  Serious KPI Failure: [97.0% - 97.9%]  Severe KPI Failure: [96.0% - 96.9%]  KPI Service Threshold: [below 96%] | 0  [1]  [2]  [3]  [4] |
| KPI2 | [Supplier System Response Times] | See Paragraph 3 of Part B of this Annex |  | Target Performance Level: [X] seconds  Minor KPI Failure: [X] seconds  Serious KPI Failure: [X] seconds  Severe KPI Failure: [X] seconds  KPI Service Threshold: [X] seconds | 0  [1]  [2]  [3]  [4] |
| KPI3 | [Help Desk Response Times] | See Paragraph 4 of Part B of this Annex |  | Target Performance Level: [X] seconds  Minor KPI Failure: [X] seconds  Serious KPI Failure: [X] seconds  Severe KPI Failure: [X] seconds  KPI Service Threshold: [X] seconds | 0  [1]  [2]  [3]  [4] |
| KPI4 | [Fix Times] | See Paragraph 5 of Part B of this Annex |  | Target Performance Level: [X] minutes  Minor KPI Failure: [X] minutes  Serious KPI Failure: [X] minutes  Severe KPI Failure: [X] minutes  KPI Service Threshold: [X] minutes | 0  [1]  [2]  [3]  [4] |
| KPI5 | [Satisfaction Surveys] | See Paragraph 6 of Part B of this Annex |  | Target Performance Level: [x]%  Minor KPI Failure: [x]%-[x]%  Serious KPI Failure: [x]%-[x]%  Severe KPI Failure: [x]%-[x]%  KPI Service Threshold: below [x]% | 0  [1]  [2]  [3]  [4] |
| KPI6 | [Virtual Library Completeness] | See Paragraph 7 of Part B of this Annex |  | Target Performance Level: [x]%  Minor KPI Failure: [x]%-[x]%  Serious KPI Failure: [x]%-[x]%  Severe KPI Failure: [x]%-[x]%  KPI Service Threshold: below [x]% | 0  [1]  [2]  [3]  [4] |
| KPI7 | [Social Value KPI 1]  ***[Guidance:* *Contracting authorities should consider carefully whether the Social Value targets chosen should be KPIs or PIs. In a market with a mature understanding and offerings around Social Value, and where it is proportionate to do so, designating them as KPIs will be appropriate (i.e. allowing for Service Credits to be used as a remedy). In a less mature market, and where it is not proportionate to make them KPIs, they should be PIs (i.e. making plans for rectification the main remedy and with the ability to withhold a proportionate amount of Service Charges until the PI failure is rectified in the case of material failure.*]** | **[insert** definition] |  | Target Performance Level: [ ]  Minor KPI Failure: [ ]  Serious KPI Failure: [ ]  Severe KPI Failure: [ ]  Service Threshold: [ ] | 0  [1]  [2]  [3]  [4] |
| KPI8 | [Social Value KPI 2] | **[insert** definition] |  | Target Performance Level: [ ]  Minor KPI Failure: [ ]  Serious KPI Failure: [ ]  Severe KPI Failure: [ ]  Service Threshold: [ ] | 0  [1]  [2]  [3]  [4] |
| KPI9 | [Social Value KPI 3] | **[insert** definition] |  | Target Performance Level: [ ]  Minor KPI Failure: [ ]  Serious KPI Failure: [ ]  Severe KPI Failure: [ ]  Service Threshold: [ ] | 0  [1]  [2]  [3]  [4] |

### Subsidiary Performance Indicators

| No. | Subsidiary Performance Indicator Title | Definition | Measurement Period | Severity Levels |
| --- | --- | --- | --- | --- |
| PI1 | [Sustainability/ Efficiency indicators] | [See Schedule 2 (*Services Description*)] |  | Target Performance Level: [xx%]  Service Threshold: [xx%] |
| PI2 | [Social Value PI]  ***[Guidance: Contracting authorities should consider carefully whether the Social Value targets chosen should be KPIs or PIs. In a market with a mature understanding and offerings around Social Value, designating them as KPIs will be appropriate (i.e. allowing for Service Credits to be used as a remedy). In a less mature market, and where it is not proportionate to make them KPIs, they should be PIs (i.e. making plans for rectification the main remedy and with the ability to withhold a proportionate amount of Service Charges until the PI failure is rectified in the case of material failure.*]** | [See Schedule 2 (*Services Description*)] |  | Target Performance Level: [xx%]  Service Threshold: [xx%] |

### Optional Services

The Key Performance Indicators and Subsidiary Performance Indicators that shall apply to the Optional Services are set out below:

### Key Performance Indicators

| No. | Key Performance Indicator Title | Definition | Measurement Period | Severity Levels | Service Points | Publishable Performance Information  *[Guidance: It is HMG’s intention to publish the top KPIs in the vast majority of contracts. The Authority must select at least three KPI/PIs which shall be publishable and also must select the single most important Social Value KPI/PI, which shall be publishable (four KPIs/PIs in total).]* |
| --- | --- | --- | --- | --- | --- | --- |
| KPI1 | [ ] | [ ] |  | Target Performance Level: [ ]  Minor KPI Failure: [ ]  Serious KPI Failure: [ ]  Severe KPI Failure: [ ]  Service Threshold: [ ] | 0  [1]  [2]  [3]  [4] | [YES/NO] |

### Subsidiary Performance Indicators

| No. | Subsidiary Performance Indicator Title | Definition | Measurement Period | Severity Levels | Publishable Performance Information  *[Guidance: It is HMG’s intention to publish the top KPIs in the vast majority of contracts. The Authority must select at least three KPI/PIs which shall be publishable and also must select the single most important Social Value KPI/PI, which shall be publishable (four KPIs/PIs in total).]* |
| --- | --- | --- | --- | --- | --- |
| PI1 | [ ] | [ ] |  | Target Performance Level: [ ]  Service Threshold: [ ] | [YES/NO] |

### Mapping of Performance Indicator severity levels to ratings under Regulation 39(5) of the Procurement Regulations 2024

***[Guidance: The following table provides space to set out how the performance ratings set out in Regulation 39(5) of the Procurement Regulations 2024 are to be mapped against the severity level descriptions used for the purposes of this Contract. For example:***

***Good = Target Performance Level ([99]%)***

***Approaching Target = Minor KPI Failure ([98.0]% - [98.9]%)***

***Requires Improvement = Serious KPI Failure ([97.0]% - [97.9]%)***

***Inadequate = Severe KPI Failure ([96.0]% - [96.9]%) or below the KPI Service Threshold (below [96.0]%)***

***Other = where performance of the Supplier cannot be described as ‘Good’, ‘Approaching Target’, ‘Requires Improvement’ or ‘Inadequate’ due to any other factor(s).***

***These are indicative only and will vary depending on the nature of the procurement and Contract to be entered into. Contracting authorities should therefore carefully consider the appropriate performance metrics to be used on a case-by-case basis.]***

| Regulation 39(5) Rating | Severity Level |
| --- | --- |
| Good | [ ] |
| Approaching Target | [ ] |
| Requires Improvement | [ ] |
| Inadequate | [ ] |
| Other | [ ] |

## Part B: Definitions

1. Available
   1. The IT Environment and/or the Services shall be Available when:
      1. End Users are able to access and utilise all the functions of the Supplier System and/or the Services; and
      2. the Supplier System is able to process the Government Data and to provide any required reports within the timescales set out in the Services Description (as measured on a 24 x 7 basis); and
      3. all Performance Indicators other than Service Availability are above the KPI Service Threshold.
2. Service Availability
   1. Service Availability shall be measured as a percentage of the total time in a Service Period, in accordance with the following formula:

Service Availability % =

where:

MP = total number of minutes, excluding Permitted Maintenance, within the relevant Service Period; and

SD = total number of minutes of Service Downtime, excluding Permitted Maintenance, in the relevant Service Period.

* 1. When calculating Service Availability in accordance with this Paragraph 2:
     1. Service Downtime arising due to Permitted Maintenance that is carried out by the Supplier in accordance with Clause 9.4 (*Maintenance*) shall be subtracted from the total number of hours in the relevant Service Period; and
     2. Service Points shall accrue if:
        1. any Service Downtime occurs as a result of Emergency Maintenance undertaken by the Supplier; or
        2. where maintenance undertaken by the Supplier exceeds **[insert** number] hours in any Service Period.

1. Response Times
   1. The “**System Response Time**” is the round trip time taken to process a message or request of the IT Environment and/or the Services, and shall be measured from the moment the last packet of data which relates to a particular message is received at the external interface of the IT Environment until a response is generated and the first block of data leaves the external interface (including, for the avoidance of doubt, the time taken for any necessary processing).
   2. The Supplier System Response Time shall be the average System Response Time measured over the course of a Service Period.
2. Help Desk Response Times
   1. Measurement of Help Desk response times will be based on the time taken for a Help Desk operative to answer a call. Calls receiving an automated response or placed into a queuing system shall be deemed not to have been answered.
   2. The Supplier shall monitor the Help Desk response times and shall provide the results of such monitoring to the Authority in accordance with the provisions of Part B of this Schedule.
3. Fix Times
   1. The “**Fix Time**” of a Service Incident is the period from the time that the Service Incident has been reported to the Supplier to the point of its Resolution and “**Resolution**” means in relation to a Service Incident either:
      1. the root cause of the Service Incident has been removed and the Services are being provided in accordance with the Services Description and Target Performance Levels; or
      2. the Authority has been provided with a workaround in relation to the Service Incident deemed acceptable by the Authority.
   2. Fix Times for Severity 3 Service Incidents, Severity 4 Service Incidents and Severity 5 Service Incidents shall be measured in Operational Hours.

**[Optional: Worked example:** if the Operational Hours for a fault are 0800-1800, then the clock stops measuring Fix Time at 1800 in the evening and restarts at 0800 the following day).]

* 1. Fix times for Severity 1 Service Incidents and Severity 2 Service Incidents shall be measured 24x7.
  2. The Supplier shall measure Fix Times as part of its service management responsibilities and report periodically to the Authority on Fix Times as part of the Performance Monitoring Report.
  3. For the purposes of this Paragraph 5, the following expressions shall have the meanings set opposite them below:

|  |  |
| --- | --- |
| **“Operational Hours”** | In relation to any Service, the hours for which that Service is to be operational as set out in Schedule 2 (*Services Description*); |
| **“Service Incident”** | a reported occurrence of a failure to deliver any part of the Services in accordance with the Authority Requirements or the Performance Indicators; |
| **“Severity 1 Service Incident”** | a Service Incident which, in the reasonable opinion of the Authority:   1. constitutes a loss of the Service which prevents a large group of End Users from working; 2. has a critical impact on the activities of the Authority; 3. causes significant financial loss and/or disruption to the Authority; or 4. results in any material loss or corruption of Government Data;   **Non-exhaustive examples:**   1. a loss of power to a data centre causing failure of Services; or 2. a failure of the Services to provide user authentication service; |
| **“Severity 2 Service Incident”** | a Service Incident which, in the reasonable opinion of the Authority has the potential to:   1. have a major (but not critical) adverse impact on the activities of the Authority and no workaround acceptable to the Authority is available; 2. have a major (but not critical) adverse impact on the activities of the Authority and no workaround acceptable to the Authority is available; or 3. cause a financial loss and/or disruption to the Authority which is more than trivial but less severe than the significant financial loss described in the definition of a Severity 1 Service Failure;   **Non-exhaustive examples:**   1. corruption of organisational database tables; or 2. loss of ability to update Government Data. |
| **“Severity 3 Service Incident”** | a Service Incident which, in the reasonable opinion of the Authority has the potential to:   1. have a major adverse impact on the activities of the Authority which can be reduced to a moderate adverse impact due to the availability of a workaround acceptable to the Authority; or 2. have a moderate adverse impact on the activities of the Authority;   **Non-exhaustive example:**   1. inability to access data for a class of customers; |
| **“Severity 4 Service Incident”** | a Service Incident which, in the reasonable opinion of the Authority has the potential to have a minor adverse impact on the provision of the Services to End Users;  **Non-exhaustive example:**   1. inability to access data for a single customer; and |
| **“Severity 5 Service Incident”** | a Service Incident comprising a flaw which is cosmetic and, as such, does not undermine the End User’s confidence in the information being displayed;  **Non-exhaustive examples:**   1. spelling error; or 2. misalignment of data on screen display. |

1. Satisfaction Surveys
   1. In order to assess the level of performance of the Supplier, the Authority may undertake satisfaction surveys in respect of End Users or various groups of End Users (each such survey a “**Satisfaction Survey**”), the results of which may be reflected in the Balanced Sustainability Report. The subject matter of Satisfaction Surveys may include:
      1. the assessment of the Supplier’s performance by the End Users against the agreed Key Performance Indicators and Subsidiary Performance Indicators; and/or
      2. other suggestions for improvements to the Services.
   2. The Authority shall reflect in the Balanced Sustainability Report any aspects of the Supplier’s performance of the Services which the responses to the Satisfaction Surveys reasonably suggest are not meeting the Services Description.
2. Virtual Library Completeness
   1. The Virtual Library shall be complete where all of the information required under Schedule 20 (*Reports and Records Provisions*) (*Annex 2: Records To Upload To Virtual Library*) has been uploaded to the Virtual Library in accordance with Paragraph 2 of that Schedule.

Schedule 4

Standards

# Schedule 4: Standards

1. Definitions
   1. In this Schedule, the following definitions shall apply:

|  |  |
| --- | --- |
| “Standards Hub” | the Government’s open and transparent standards adoption process as documented at <http://standards.data.gov.uk/>; and |
| “Suggested Challenge” | a submission to suggest the adoption of new or emergent standards in the format specified on Standards Hub. |

1. General
   1. Throughout the term of this Contract, the Parties shall monitor and notify each other of any new or emergent standards which could affect the Supplier’s provision, or the Authority’s receipt, of the Services. Any changes to the Standards, including the adoption of any such new or emergent standard, shall be agreed in accordance with the Change Control Procedure.
   2. Where a new or emergent standard is to be developed or introduced by the Authority, the Supplier shall be responsible for ensuring that the potential impact on the Supplier’s provision, or the Authority’s receipt, of the Services is explained to the Authority (in a reasonable timeframe), prior to the implementation of the new or emergent standard.
   3. Where Standards referenced conflict with each other or with Good Industry Practice, then the later Standard or best practice shall be adopted by the Supplier. Any such alteration to any Standard(s) shall require the prior written agreement of the Authority and shall be implemented within an agreed timescale.
2. Technology and Digital Services Practice
   1. The Supplier shall (when designing, implementing and delivering the Services) adopt the applicable elements of HM Government’s Technology Code of Practice as documented at <https://www.gov.uk/service-manual/technology/code-of-practice.html>.
3. Open Data Standards & Standards Hub
   1. The Supplier shall comply to the extent within its control with UK Government’s Open Standards Principles as documented at <https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles>, as they relate to the specification of standards for software interoperability, data and document formats in the IT Environment.
   2. Without prejudice to the generality of Paragraph 2.2, the Supplier shall, when implementing or updating a technical component or part of the Software or Supplier Solution where there is a requirement under this Contract or opportunity to use a new or emergent standard, submit a Suggested Challenge compliant with the UK Government’s Open Standards Principles (using the process detailed on Standards Hub and documented at <http://standards.data.gov.uk/>). Each Suggested Challenge submitted by the Supplier shall detail, subject to the security and confidentiality provisions in this Contract, an illustration of such requirement or opportunity within the IT Environment, Supplier Solution and Government’s IT infrastructure and the suggested open standard.
   3. The Supplier shall ensure that all documentation published on behalf of the Authority pursuant to this Contract is provided in a non-proprietary format (such as PDF or Open Document Format (ISO 26300 or equivalent)) as well as any native file format documentation in accordance with the obligation under Paragraph 4.1 to comply with the UK Government’s Open Standards Principles, unless the Authority otherwise agrees in writing.
4. Technology Architecture Standards
   1. The Supplier shall produce full and detailed technical architecture documentation for the Supplier Solution in accordance with Good Industry Practice. If documentation exists that complies with the Open Group Architecture Framework 9.2 or its equivalent, then this shall be deemed acceptable.
5. Accessible Digital Standards
   1. The Supplier shall comply with (or with equivalents to):
      1. the World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI) Web Content Accessibility Guidelines (WCAG) 2.2 Conformance Level AA and future versions as updated from time to time; and
      2. ISO/IEC 13066-1: 2011 Information Technology – Interoperability with assistive technology (AT) – Part 1: Requirements and recommendations for interoperability.
6. Service Management Software & Standards
   1. Subject to Paragraphs 2 to 4 (inclusive), the Supplier shall reference relevant industry and HM Government standards and best practice guidelines in the management of the Services, including the following and/or their equivalents:
      1. ITIL v4;
      2. ISO/IEC 20000-1 2018 “Information technology — Service management – Part 1”;
      3. ISO/IEC 20000-2 2019 “Information technology — Service management – Part 2”;
      4. ISO 10007: 2017 “Quality management systems – Guidelines for configuration management”; and
      5. ISO 22313:2020 “Security and resilience. Business continuity management systems. Guidance on the use of ISO 22301” and, ISO/IEC 27031:2011 and ISO 22301:2019.
   2. For the purposes of management of the Services and delivery performance the Supplier shall make use of Software that complies with Good Industry Practice including availability, change, incident, knowledge, problem, release & deployment, request fulfilment, service asset and configuration, service catalogue, service level and service portfolio management. If such Software has been assessed under the ITIL Software Scheme as being compliant to “Bronze Level”, then this shall be deemed acceptable.
7. Sustainability
   1. The Supplier shall comply with the sustainability requirements set out in Annex 1 to this Schedule 4.
8. Hardware Safety Standards
   1. The Supplier shall comply with those BS or other standards relevant to the provision of the Services, including the following or their equivalents:
      1. any new hardware required for the delivery of the Services (including printers), shall conform to BS EN IEC 62368-1:2020+A11:2020 or subsequent replacements. In considering where to site any such hardware, the Supplier shall consider the future working user environment and shall position the hardware sympathetically, wherever possible;
      2. any new audio, video and similar electronic apparatus required for the delivery of the Services, shall conform to the following standard: BS EN IEC 62368-1:2020+A11:2020 or any subsequent replacements;
      3. any new laser printers or scanners using lasers, required for the delivery of the Services, shall conform to either of the following safety Standards: BS EN 60825-1:2014 or any subsequent replacements; and
      4. any new apparatus for connection to any telecommunication network, and required for the delivery of the Services, shall conform to the following safety Standard: BS EN 62949:2017 or any subsequent replacements.
   2. Where required to do so as part of the Services, the Supplier shall perform electrical safety checks in relation to all equipment supplied under this Contract in accordance with the relevant health and safety regulations.

## Annex 1: Sustainability

**[*Guidance****:* ***As set out in the MSC Guidance, this Annex 1*** ***has been designed to provide a starting point for sustainability requirements in any procurement. Authorities are expected to tailor the annex to their specific procurements. Authorities may also choose whether or not to include any paragraph or sub-paragraph marked optional. Authorities will want to select and amend those requirements which are appropriate for their Contract, ensuring that these are relevant and proportional to the subject matter of the Contract. Authorities may want to consider using some or all of these paragraphs when there are key sustainability benefits or risks that need to be managed and/or for higher value/larger Suppliers and/or Contracts. Authorities should also note that some obligations, such as compliance with the Authority’s sustainability requirements, for example net zero commitments or EDI, will require the Authority to provide the requirements to the Supplier.*]**

1. Definitions
   1. In this Annex 1, the following definitions shall apply:

|  |  |
| --- | --- |
| “Permitted Item” | those items which are permissible under this Contract to the extent set out in Table B of this Annex 1; |
| “Prohibited Items” | those items which are not permissible under this Contract as set out at Table A of this Annex 1; |
| “Sustainability Reports” | written reports to be completed by the Supplier containing the information outlined in Table C of this Annex 1; and |
| “Waste Hierarchy” | prioritisation of waste management in the following order of preference as set out in the Waste (England and Wales) Regulation 2011:   1. Prevention; 2. Preparing for re-use; 3. Recycling; 4. Other Recovery; and 5. Disposal. |

1. Public Sector Equality Duty
   1. In addition to legal obligations, where the Supplier is providing a Service to which the Public Sector Equality duty applies, the Supplier shall support the Authority in fulfilling its Public Sector Equality duty under S149 of the Equality Act 2010 by ensuring that it fulfils its obligations under the Contract in a way that seeks to:
      1. eliminate discrimination, harassment or victimisation and any other conduct prohibited by the Equality Act 2010; and
      2. advance:
         1. equality of opportunity; and
         2. good relations,

between those with a protected characteristic (age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex, sexual orientation, and marriage and civil partnership) and those who do not share it.

* 1. [**Optional:** In delivering the Service, the Supplier will comply with the Authority’s equality, diversity and inclusion requirements, to be provided to the Supplier by the Authority.]
  2. [**Optional:** The Supplier shall ensure that it fulfils its obligations under the Contract in a way that does not discriminate against individuals because of socio-economic background, working pattern or having parental or other caring responsibilities.]

1. Environmental Requirements
   1. The Supplier must perform its obligations meeting in all material respects the requirements of all applicable Laws regarding the environment.
   2. The Supplier warrants that it has obtained relevant Environment Management System (EMS) certified to ISO 14001 or an equivalent certification from a UKAS accredited body and shall comply with and maintain certification requirements throughout the Term.
   3. In performing its obligations under the Contract the Supplier shall, where applicable to the Contract, to the reasonable satisfaction of the Authority:
      1. demonstrate low carbon resource efficiency, including minimising the use of resources and responding promptly to the Authority’s reasonable questions;
      2. prioritise waste management in accordance with the Waste Hierarchy as set out in Law;
      3. be responsible for ensuring that any waste generated by the Supplier and sent for recycling, disposal or other recovery as a consequence of this Contract is taken by a licensed waste carrier to an authorised site for treatment or disposal and that the disposal or treatment of waste complies with the law;
      4. ensure that it and any third parties used to undertake recycling disposal or other recovery as a consequence of this Contract do so in a legally compliant way, and can demonstrate that reasonable checks are undertaken to ensure this on a regular basis and provide relevant data and evidence of recycling, recovery and disposal;
      5. in circumstances that a permit, licence or exemption to carry or send waste generated under this Contract is revoked, the Supplier shall cease to carry or send waste or allow waste to be carried by any Subcontractor until authorisation is obtained from the Environment Agency; minimise the release of greenhouse gases (including carbon dioxide emissions), air pollutants, volatile organic compounds and other substances damaging to health and the environment; and
      6. reduce and minimise carbon emissions by taking into account factors including, but not limited to, the locations from which materials are sourced, the transport of materials, the locations from which the work force are recruited and emissions from offices and on-site equipment.
   4. In performing its obligations under the Contract, the Supplier shall to the reasonable satisfaction of the Authority (where: (i) the anticipated Charges in any Contract Year are above £5 million per annum (excluding VAT); (ii) this is a public contract, other than a special regime contract under the Procurement Act 2023; and (iii) it is related to and proportionate to the contract in accordance with PPN 006), publish and maintain a credible Carbon Reduction Plan in accordance with PPN 006.
   5. The Supplier shall not provide to the Authority Goods or Deliverables which comprise wholly or partly of Prohibited Items unless such item is a Permitted Item.
   6. The Supplier shall not use anything which comprises wholly or partly of the Prohibited Items to provide the Services under this Contract unless:
      1. it is a Permitted Item; or
      2. the use is primarily related to the management of the Supplier’s own facilities or internal operations as opposed to the provision of Services.
   7. [**Optional:** The Supplier must have a documented management system and controls in place to manage the environmental impacts of delivering the Services.]
   8. [**Optional:** The Supplier shall ensure that any Services are designed, sourced and delivered in a manner which is environmentally and socially responsible.]
   9. [**Optional:** In delivering the Services, the Supplier must comply with the Authority’s sustainability requirements, to be provided to the Supplier by the Authority.]
   10. [**Optional:** In performing its obligations under the Contract, the Supplier shall to the reasonable satisfaction of the Authority:
       1. [**Optional:** demonstrate that the whole life cycle impacts (including end of use) associated with the Services that extend beyond direct operations into that of the supply chain have been considered and reduced];
       2. [**Optional:** minimise the consumption of resources and use them efficiently (including water and energy), working towards a circular economy including designing out waste and non-renewable resources, using re-use and closed loop systems];
       3. [**Optional:** demonstrate protection of the environment including understanding and reduction of biosecurity risks (which include risks to plant and tree health from harmful pests and diseases), and reducing and eliminating hazardous/harmful substances to the environment and preventing pollution];
       4. [**Optional:** enhance the natural environment and connecting communities with the environment]; and
       5. [**Optional:** achieve continuous improvement in environmental (and social) performance.]
   11. [**Optional:** The Supplier shall inform the Authority within one Working Day in the event that a permit, licence or exemption to carry or send waste generated under this Contract is revoked.]
   12. **[Guidance: *Insert any other environmental requirement the Authority wishes to add, e.g. those in line with the Government Greening Commitments, the Greening government: ICT and digital services strategy 2020 to 2025 and point 12 of the Technology Code of Practice.*]**
   13. The Supplier shall meet the applicable Government Buying Standards applicable to Services which can be found online at:

<https://www.gov.uk/government/collections/sustainable-procurement-the-government-buying-standards-gbs>.

1. Supplier Code of Conduct
   1. In February 2019, HM Government published a Supplier Code of Conduct setting out the standards and behaviours expected of suppliers who work with government which can be found online at:

<https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1163536/Supplier_Code_of_Conduct_v3.pdf>

* 1. The Authority expects to meet, and expects its suppliers and subcontractors to meet, the standards set out in that Code.

1. Reporting Requirements
   1. The Supplier shall comply with reasonable requests by the Authority for information evidencing compliance:
      1. with Paragraphs 2.1, 3.1 to 3.6, 3.13 and 4 of this Annex 1 within [fourteen (14)] days of such request; and
      2. With Paragraphs 2.2, 2.3 and 3.7 to 3.12 of this Annex 1 within [thirty (30) days] of such request[.]/[,

provided that such requests are limited to [two] per Contract Year.]

* 1. The Supplier shall complete the Sustainability Report in relation to its provision of the Services under this Contract and provide the Sustainability Report to the Authority on the date and frequency outlined in Table C of this Annex 1.

### Table A – Prohibited Items

|  |  |
| --- | --- |
| The following consumer single use plastics are Prohibited Items: | Catering   1. Single use sachets e.g. coffee pods, sauce sachets, milk sachets 2. Take away cutlery 3. Take away boxes and plates 4. Cups made wholly or partially of plastic 5. Straws 6. Stirrers 7. Water bottles |
| Facilities   1. Single use containers e.g. hand soap, cleaning products 2. Wipes containing plastic |
| Office Supplies   1. Plastic envelopes 2. Plastic wrapping for brochures 3. Paper or card which is bleached with chlorine |
| Packaging   1. Single use plastic packaging from deliveries where avoidable e.g. shrink wrapped packaging from office supplier or facilities products. 2. Single use carrier bags |
| Authority Specific Prohibitions | [Authority to consider other items outside of the Cabinet Office 2020 commitment to be prohibited]  [Conflict minerals as defined by the <https://www.gov.uk/guidance/conflict-minerals>, E.g. non-recyclable plastic pens] |
| Project specific Prohibitions | **[Insert** items specific to the project which you wish to prohibit use of for sustainability reasons] |

### Table B – Permitted Items

|  |  |
| --- | --- |
| Authority Permitted Items | [Authority to consider whether there are other items which it may wish to expressly authorise] |
| Project Specific Permitted Items | [A market consultation should be undertaken before issuing the ITT to ensure that necessary items are not precluded from this project.  Items should be permitted for operational, technical, economic, or environmental reasons. The Authority should include the circumstances that the prohibition should not apply if the exception should apply in only limited instances.] |

### Table C – Sustainability Reports

**[*Guidance: All reports and the content of these reports in Table C are optional. Authorities will want to select and amend those reports and requirements which are appropriate for their Contract, ensuring that these are relevant and proportional to the subject matter of the Contract and do not create unnecessary burdens upon the Supplier.]***

| **Sustainability Report Name** | **Content of Report** | **Frequency of Report** |
| --- | --- | --- |
| [Sustainability - General] | [as proportionate and relevant to the Contract, the key sustainability impacts identified; the sustainability improvements planned or delivered; and the risks to the Services of climate change, including mitigation, adaptation and continuity plans employed by the Supplier in response to those risks]. | [On the anniversary of the Effective Date] |
| [Waste Created] | [By type of material the weight of waste categories by each means of disposal in the Waste Hierarchy with separate figures for disposal by incineration and landfill.] | [Before contract award and on the anniversary of the Effective Date.] |
| [Waste Permits] | [Copies of relevant permits and exemptions for waste, handling, storage and disposal.] | [Before the Effective Date, on the anniversary of the Effective Date and within ten (10) Working Days if there is any change or renewal to license or exemption to carry, store or dispose waste] |
| [Greenhouse Gas Emissions] | [Detail the Scope 1 and Scope 2 GHG emissions associated with the delivery of the contract.  Scope 3 emissions to be reported as required (Optional)  Emissions reporting should be in accordance with established best practice and internationally accepted standards.  Greenhouse gas reporting from emissions sources (Scope 1, Scope 2 and Scope 3), and specific activities as requested by the Authority. This may include activities such as transportation, energy use and waste disposal.] | [On the anniversary of the Effective Date] |
| [Water Use] | [Volume in metres cubed.] | [On the anniversary of the Effective Date] |
| [Other] | [ ] | [ ] |

Schedule 5

Security Management

# Schedule 5: Security Management

***[Guidance: This Schedule contains two options for the Security Management Schedule, i.e.:***

1. ***Part A: Authority-led Assurance; or***
2. ***Part B: Supplier-led Assurance.***

***The Authority should select which option it wants to use in the Front Sheet and delete the other option from the Schedule. The option that is left will then apply.]***

## Part A: Authority-led Assurance

1. Authority Options

Where the Authority has selected an option in the table below, the Supplier must comply with the requirements relating to that option set out in the relevant Paragraph:

|  |  |  |
| --- | --- | --- |
| * 1. **Authority Security Policies** (see Paragraph 5) | | |
| * 1. The Authority requires the Supplier to comply with the following policies relating to security management: * [**List Authority security policies with which the Supplier and Subcontractors must comply]** | | * 1. ☐ |
| * 1. **Secure by Design Principles** (see Paragraph 14.6) | | |
| * 1. The Authority waives the requirement for the Security Management Plan to include an assessment of the Supplier Information Management System against the table in Appendix 5 (*Secure by Design Principles Evaluation Table*). | | * 1. ☐ |
| * 1. **Locations** (see Paragraph 1 of the Security Requirements) | | |
| * 1. The Supplier and Subcontractors may store, access or Handle Government Data in: | * 1. the United Kingdom only | * 1. ☐ |
| * 1. any territory as permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State) | * 1. ☐ |
| * 1. anywhere in the world not prohibited by the Authority | * 1. ☐ |
| * 1. **Support Locations** (see Paragraph 1 of the Security Requirements) | | |
| * 1. The Supplier and Subcontractors may operate Support Locations in: | * 1. the United Kingdom only | * 1. ☐ |
| * 1. any territory as permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State) | * 1. ☐ |
| * 1. anywhere in the world not prohibited by the Authority | * 1. ☐ |
| * 1. **Development Activity** (see Appendix 2 (*Security Requirements for Development*) | | |
| * 1. The Authority requires the Supplier to undertake Development Activity under this Contract and, as a consequence, Appendix 2 (*Security Requirements for Development*) applies | | * 1. ☐ |
| * 1. **Locations for Development Activity** (applies only if the option relating to Development Activities is selected; see Paragraph 1 of the Security Requirements) | |  |
| * 1. The Supplier and Subcontractors may undertake Development Activity in: | * 1. the United Kingdom only | * 1. ☐ |
|  | * 1. any territory as permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State) | * 1. ☐ |
|  | * 1. anywhere in the world not prohibited by the Authority | * 1. ☐ |

1. Definitions

***[Guidance: Please note the following defined terms used within this Schedule can be found within Schedule 1 (Definitions): Assets, Authority Equipment, Authority Premises, Authority System, Code, Developed System, EEA, Government Data, Handle, Key Subcontractor, Malicious Software, Security Requirements, Security Requirements for Development, Sites.]***

|  |  |
| --- | --- |
| * 1. **"Anti‑virus Software"** | * 1. software that:      1. protects the Supplier Information Management System from the possible introduction of Malicious Software;      2. scans for and identifies possible Malicious Software in the Supplier Information Management System;      3. if Malicious Software is detected in the Supplier Information Management System, so far as possible:         1. prevents the harmful effects of the Malicious Software; and         2. removes the Malicious Software from the Supplier Information Management System; |
| * 1. **"Authority-led Assurance"** | the assessment of the Supplier Information Management System in accordance with Paragraph 15 by the Authority or an independent information risk manager or other qualified professional appointed by the Authority; |
| * 1. **"Backup and Recovery Plan"** | * 1. the section of the Security Management Plan setting out the Suppliers' and Subcontractors' plans for the back and recovery of any Government Data they Handle; |
| * 1. **"Breach Action Plan"** | * 1. a plan prepared under Paragraph 16.3 of the Security Requirements addressing any Breach of Security; |
| * 1. **"Breach of Security"** | * 1. the occurrence of:      1. any unauthorised access to or use of the Services, the Authority Premises, the Sites, the Supplier Information Management System and/or any information or data used by the Authority, the Supplier or any Subcontractor in connection with this Contract, including the Government Data and the Code;      2. the loss (physical or otherwise), corruption and/or unauthorised disclosure of any information or data, including copies of such information or data, used by the Authority, the Supplier or any Subcontractor in connection with this Contract, including the Government Data and the Code;      3. any part of the Supplier Information Management System ceasing to be compliant with the Certification Requirements;      4. the installation of Malicious Software in the:         1. Supplier Information Management System;         2. Development Environment; or         3. Developed System; and/or      5. any loss of operational efficiency or failure to operate to specification as the result of the installation or operation of Malicious Software in the:         1. Supplier Information Management System;         2. Development Environment; or         3. Developed System; and      6. includes any attempt to undertake the activities listed in sub-Paragraph (a) of this definition where the Supplier has reasonable grounds to suspect that attempt:         1. was part of a wider effort to access information and communications technology operated by or on behalf of Central Government Bodies; or         2. was undertaken, or directed by, a state other than the United Kingdom; |
| * 1. **"Certification Requirements"** | * 1. the requirements set out in Paragraph 13.4; |
| * 1. **"CHECK Scheme"** | * 1. the NCSC's scheme under which approved companies can conduct authorised penetration tests of public sector and critical national infrastructure systems and networks; |
| * 1. **"CHECK Service Provider"** | * 1. a company which, under the CHECK Scheme:      1. has been certified by the National Cyber Security Centre;      2. holds "Green Light" status; and      3. is authorised to provide the IT Health Check services required by Paragraph 12 of the Security Requirements; |
| * 1. **"CHECK Team Leader"** | * 1. an individual with a CHECK Scheme team leader qualification issued by the NCSC; |
| * 1. **"CHECK Team Member"** | * 1. an individual with a CHECK Scheme team member qualification issued by the NCSC; |
| * 1. **"Code Review"** | * 1. a periodic review of the Code by manual or automated means to:      1. identify and fix any bugs; and      2. ensure the Code complies with         1. the requirements of this Schedule 5 (*Security Management*); and         2. the Secure Development Guidance; |
| * 1. **"Code Review Plan"** | * 1. the document agreed with the Authority under Paragraph 5.2 of the Security Requirements for Development setting out the requirements for, and frequency of, Code Reviews; |
| * 1. **"Code Review Report"** | * 1. a report setting out the findings of a Code Review; |
| * 1. **"Cyber Essentials"** | * 1. the Cyber Essentials certificate issued under the Cyber Essentials Scheme; |
| * 1. **"Cyber Essentials Plus"** | * 1. the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme; |
| * 1. **"Cyber Essentials Scheme"** | * 1. the Cyber Essentials scheme operated by the National Cyber Security Centre; |
| * 1. **"Data Migration Plan"** | * 1. the plan for the migration of the Government Data to the Authority and/or the Replacement Supplier (as required by the Authority) required by Paragraph 17 of the Security Requirements; |
| * 1. **"Development Activity"** | * 1. any activity relating to the development, deployment maintenance and upgrading of the Developed System, including:      1. coding;      2. testing;      3. code storage; and      4. deployment; |
| * 1. **"Development Environment"** | * 1. any information and communications technology system and the Sites forming part of the Supplier Information Management System that the Supplier or its Subcontractors will use to provide the Development Activity; |
| * 1. **"End-user Device"** | * 1. any personal computers, laptops, tablets, terminals, smartphones or other portable electronic device provided by the Supplier or a Subcontractor and used in the provision of the Services; |
| * 1. **"Email Service"** | * 1. a service that will send, or can be used to send, emails from the Authority's email address or otherwise on behalf of the Authority; |
| * 1. **"Expected Behaviours"** | * 1. the expected behaviours set out and updated from time to time in the Government Security Classification Policy, currently found at paragraphs 12 to 16 and in the table below paragraph 16 of <https://www.gov.uk/government/publications/government-security-classifications/guidance-11-working-at-official-html>; |
| * 1. **"Government Data Register"** | * 1. the register of all Government Data the Supplier, or any Subcontractor, receives from or creates for the Authority, produced and maintained in accordance with Paragraph 18 of the Security Requirements; |
| * 1. **"Government Security Classification Policy"** | * 1. the policy, as updated from time to time, establishing an administrative system to protect information assets appropriately against prevalent threats, including classification tiers, protective security controls and baseline behaviours, the current version of which is found at [https://www.gov.uk/ government/publications/government-security-classifications](https://www.gov.uk/government/publications/government-security-classifications/guidance-11-working-at-official-html); |
| * 1. **"Higher-risk Subcontractor"** | * 1. a Subcontractor that Handles Government Data, where that data includes either:      1. the Personal Data of 1000 or more individuals in aggregate during the period between the first Operational Service Commencement Date and the date on which this Contract terminates in accordance with Clause 4.1.2; or      2. any part of that Personal Data includes any of the following:         1. financial information (including any tax and/or welfare information) relating to any person;         2. any information relating to actual or alleged criminal offences (including criminal records);         3. any information relating to children and/or vulnerable persons;         4. any information relating to social care;         5. any information relating to a person's current or past employment; or         6. Special Category Personal Data; or      3. the Authority in its discretion, designates a Subcontractor as a Higher- risk Subcontractor:         1. in any procurement document related to this Contract; or         2. during the Term; |
| * 1. **"HMG Baseline Personnel Security Standard"** | * 1. the employment controls applied to any individual member of the Supplier Personnel that performs any activity relating to the provision or management of the Services, as set out in "HMG Baseline Personnel Standard", Version 7.0, June 2024 (<https://www.gov.uk/government/publications/government-baseline-personnel-security-standard>), as that document is updated from time to time; |
| * 1. **"Independent Security Adviser"** | the independent and appropriately qualified and experienced security architect or expert appointed under Paragraph 19; |
| * 1. **"ISO Certification"** | * 1. either of the following certifications when issued by a UKAS-recognised Certification Body:      1. ISO/IEC27001:2013, where the certification was obtained before November 2022, but only until November 2025; and      2. ISO/IEC27001:2022 in all other cases; |
| * 1. **"IT Health Check"** | * 1. testing of the Supplier Information Management System by a CHECK Service Provider; |
| * 1. **"Key Sub‑contractor Default"** | * 1. has the meaning set out in Paragraph 10.5; |
| * 1. **"Medium-risk Subcontractor"** | * 1. a Subcontractor that Handles Government Data, [where that data      1. includes the Personal Data of between 100 and 999 individuals (inclusive) in the period between the first Operational Service Commencement Date and the date on which this Contract terminates in accordance with Clause 4.1.2; and      2. does not include Special Category Personal Data]; |
| * 1. **"Modules Register"** | * 1. the register of Third‑party Software Modules required by Paragraph 7.3 of the Security Requirements for Development; |
| * 1. **"NCSC"** | * 1. the National Cyber Security Centre or any replacement or successor body carrying out the same function; |
| * 1. **"NCSC Cloud Security Principles"** | * 1. the NCSC's document "Implementing the Cloud Security Principles" as updated or replaced from time to time and found at <https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles>; |
| * 1. **"NCSC Device Guidance"** | * 1. the NCSC's document "Device Security Guidance", as updated or replaced from time to time and found at <https://www.ncsc.gov.uk/collection/device-security-guidance>; |
| * 1. **"NCSC Protecting Bulk Personal Data Guidance"** | * 1. the NCSC's document "Protecting Bulk Personal Data", as updated or replaced from time to time and found at <https://www.ncsc.gov.uk/collection/protecting-bulk-personal-data>; |
| * 1. **"NCSC Secure Design Principles"** | * 1. the NCSC's document "Secure Design Principles", as updated or replaced from time to time and found at <https://www.ncsc.gov.uk/collection/cyber-security-design-principles/cyber-security-design-principles>; |
| * 1. **"OWASP"** | * 1. the Open Web Application Security Project Foundation; |
| * 1. **"OWASP Secure Coding Practice"** | * 1. the Secure Coding Practices Quick Reference Guide published by OWASP, as updated or replaced from time to time and found at <https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/>; |
| * 1. **"OWASP Top Ten"** | * 1. the list of the most critical security risks to web applications published annually by OWASP and found at <https://owasp.org/www-project-top-ten/>; |
| * 1. **"Privileged User"** | * 1. a user with system administration access to the Supplier Information Management System, or substantially similar access privileges; |
| * 1. **"Prohibited Activity"** | * 1. the storage, access or Handling of Government Data prohibited by a Prohibition Notice; |
| * 1. **"Prohibition Notice"** | * 1. a notice issued under Paragraph 1.11 of the Security Requirements; |
| * 1. **"Protective Monitoring System"** | * 1. the system implemented by the Supplier and its Subcontractors under Paragraph 14.1 of the Security Requirements to monitor and analyse access to and use of the Supplier Information Management System, the Development Environment, the Government Data and the Code; |
| * 1. **"RAP Trigger"** | * 1. the occurrence of one of the events set out in Paragraph 18.1; |
| * 1. **"Register of Sites, Support Locations and Third-party Tools"** | * 1. the part of the Security Management Plan setting out, in respect of Sites, Support Locations and Third-party Tools:      1. the Sites, Support Locations and Third-party Tools that the Supplier will use to Handle Government Data or provide the Services;      2. the nature of the activity performed at the Site or Support Location or by the Third-party Tool in respect of the Government Data;      3. in respect of each entity providing a Site, Support Location or Third-party Tool, its:         1. full legal name;         2. trading name (if any)         3. country of registration;         4. registration number (if applicable); and         5. registered address; |
| * 1. **"Relevant Activities"** | * 1. those activities specified in Paragraph 1.1 of the Security Requirements; |
| * 1. **"Relevant Certifications"** | * + 1. in the case of the Supplier, any SIMS Subcontractor and any Key Sub-contractor::        1. either:           1. an ISO Certification in respect of the Supplier Information Management System; or           2. where the Supplier Information Management System is included within the scope of a wider ISO Certification, that ISO Certification; and        2. Cyber Essentials Plus;     2. in the case of any Higher-risk Subcontractor, either:        1. an ISO Certification in respect of that part of the Supplier Information Management System provided by the Higher-risk Subcontractor;        2. where the that part of the Supplier Information Management System provided by the Higher-risk Subcontractor is included within the scope of a wider ISO Certification, that ISO Certification; or        3. Cyber Essentials Plus; and     3. in the case of any Medium-risk Subcontractors, Cyber Essentials.   (or equivalent certifications); |
| * 1. **"Relevant Convictions"** | * 1. any previous or pending prosecution, conviction or caution (excluding any spent conviction under the Rehabilitation of Offenders Act 1974) relating to offences involving dishonesty, terrorism, immigration, firearms, fraud, forgery, tax evasion, offences against people (including sexual offences), or any other offences relevant to Services as the Authority may specify; |
| * 1. **"Remediation Action Plan"** | * 1. the plan prepared by the Supplier in accordance with Paragraph 19; |
| * 1. **"Remote Location"** | * 1. a location other than a Supplier's or a Subcontractor's Site; |
| * 1. **"Remote Working"** | * 1. the provision or management of the Services by Supplier Personnel from a location other than a Supplier's or a Subcontractor's Site; |
| * 1. **"Remote Working Policy"** | * 1. the policy prepared and approved under Paragraph 3.8 of the Security Requirements and forming part of the Security Management Plan under which Supplier Personnel are permitted to undertake Remote Working; |
| * 1. **"Required Changes Register"** | * 1. the register recording each of the changes that the Supplier proposes to the Supplier Information Management System or the Security Management Plan together with:      1. the details of any approval of the change provided by the Authority, including any conditions or limitations on that approval; and      2. the date:         1. the date by which the change it to be implemented; and         2. the date on which the change was implemented; |
| * 1. **"Residual Risk Statement"** | * 1. a notice issued by the Authority that:      1. sets out the information risks associated with using the Supplier Information Management System; and      2. confirms that the Authority:         1. is satisfied that the identified risks have been adequately and appropriately addressed; and         2. that the residual risks are understood and accepted by the Authority; |
| * 1. **"Risk Management Approval Statement"** | * 1. the statement issued by the Authority under Paragraph 15.7 following the Authority-led Assurance of the Supplier Information Management System; |
| * 1. **"Secure by Design Principles"** | * 1. the Secure by Design Principles issued by the Cabinet Office, as updated or replaced from time-to-time, currently found at <https://www.security.gov.uk/policy-and-guidance/secure-by-design/principles/>; |
| * 1. **"Secure Development Guidance"** | * 1. the Supplier's secure coding policy required under its ISO27001 Relevant Certification; |
| * 1. **"Secure Location"** | * 1. has the meaning given to that term in Paragraph 2.1(a) of Appendix 1 (*Security Requirements*); |
| * 1. **"Security Controls"** | * 1. the security controls set out and updated from time to time in the Government Security Classification Policy, currently found at Paragraph 12 of <https://www.gov.uk/government/publications/government-security-classifications/guidance-15-considerations-for-security-advisors-html>; |
| * 1. **"Security Management Plan"** | * 1. the document prepared in accordance with the requirements of Paragraph 14 and in the format, and containing the information, specified in [**insert cross-reference to guidance**]; |
| * 1. **"Security Test"** | * + 1. an IT Health Check; or     2. a Supplier Security Test; |
| * 1. **"Security Working Group"** | the Board established under Paragraph 8 or Schedule 17 (*Governance*), as applicable; |
| * 1. **"SIMS Subcontractor"** | * 1. a Subcontractor designated by the Authority that provides or operates the whole, or a substantial part, of the Supplier Information Management System; |
| * 1. **"SMP Subcontractor"** | * 1. a Subcontractor that provides cloud-based services on a "one to many" basis, where such Subcontractor will not contract other than on their own contractual terms; |
| * 1. **"Statement of Information Risk Appetite"** | * 1. the statement provided by the Authority under Paragraph 14.1 setting out:      1. the nature and level of risk that the Supplier accepts from the operation of the Supplier Information Management System; and      2. the specific legal and regulatory requirements with which the Supplier must comply when Handling Government Data; |
| * 1. **"Subcontractor"** | * 1. for the purposes of this Schedule 5 (*Security Management*) only, any individual or entity that:      1. forms part of the supply chain of the Supplier; and      2. has access to, hosts, or performs any operation on or in respect of the Supplier Information Management System, the Development Environment, the Code and the Government Data,   2. and this definition shall apply to this Schedule 5 in place of the definition of Sub-contractor in Schedule 1 *(Definitions)*; |
| * 1. **"Subcontractors' Systems"** | the information and communications technology system used by a Subcontractor in implementing and performing the Services, including:   * + 1. the Software;     2. the Supplier Equipment;     3. configuration and management utilities;     4. calibration and testing tools;     5. and related cabling; but   does not include the Authority System; |
| * 1. **"Supplier Information Management System"** | those parts of Wider Information Management System that the Authority has determined in accordance with Paragraph 11, following consultation with the Supplier, shall be subject to Authority‑led Assurance; |
| * 1. **"Supplier Personnel"** | * 1. for the purposes of this Schedule 5 (*Security Management*) only, any individual engaged, directly or indirectly, or employed by the Supplier or any Subcontractor (as that term is defined for the purposes of this Schedule 5 (*Security Management*)), in the management or performance of the Supplier's obligations under this Contract, and this definition shall apply to this Schedule 5 (*Security Management*) in place of the definition of Supplier Personnel in Schedule 1 (*Definitions*); |
| * 1. **"Support Location"** | * 1. a place or facility where or from which individuals may access or Handle the Code or the Government Data; |
| * 1. **"Support Register"** | * 1. the register of all hardware and software used to provide the Services produced and maintained in accordance with Paragraph 5 of the Security Requirements; |
| * 1. **"Third-party Software Module"** | * 1. any module, library or framework that:      1. is not produced by the Supplier or a Subcontractor as part of the Development Activity; and      2. either:         1. forms, or will form, part of the Code; or         2. is, or will be, accessed by the Developed System during its operation; |
| * 1. **"Third-party Tool"** | * 1. any Software used by the Supplier or a Subcontractor by which the Code or the Government Data is accessed, analysed or modified, or some form of operation is performed on it; |
| * 1. **"UKAS"** | * 1. the United Kingdom Accreditation Service; |
| * 1. **"UKAS-recognised Certification Body"** | * + 1. an organisation accredited by UKAS to provide certification of ISO/IEC27001:2013 and/or ISO/IEC27001:2022; or     2. an organisation accredited to provide certification of ISO/IEC27001:2013 and/or ISO/IEC27001:2022 by a body with the equivalent functions as UKAS in a state with which the UK has a mutual recognition agreement recognising the technical equivalence of accredited conformity assessment; and |
| * 1. **"Wider Information Management System"** | * + 1. any:        1. information assets,        2. IT systems,        3. IT services; or Sites   that the Supplier or any Subcontractor will use to Handle, or support the Handling of, Government Data and provide, manage or support the provision of, the Services; and   * + 1. the associated information management system, including all relevant:        1. organisational structure diagrams,        2. controls,        3. policies,        4. practices,        5. procedures,        6. processes; and        7. resources. |

1. Introduction
2. This Schedule 5 (*Security Management*) sets out:
   1. the Authority's decision on where the Supplier may:
      1. store, access or Handle Government Data;
      2. undertake the Development Activity;
      3. host the Development Environment; and
      4. locate Support Locations,

(in Paragraph 1);

* 1. the principles of security that apply to this Contract (in Paragraph 4);
  2. the requirement to obtain a Risk Management Approval Statement (in Paragraphs 6 and 15);
  3. the annual confirmation of compliance to be provided by the Supplier (in Paragraph 7);
  4. the governance arrangements for security matters, where these are not otherwise specified in Schedule 17 (*Governance*) (in Paragraph 8);
  5. access to personnel (in Paragraph 9);
  6. obligations in relation to Subcontractors (in Paragraph 10);
  7. the responsibility of the Authority to determine the Supplier Information Management System that will be subject to Authority-led Assurance (in Paragraph 11);
  8. the Certification Requirements (in Paragraph 13);
  9. the development, monitoring and updating of the Security Management Plan by the Supplier(in Paragraphs 14, 15 and 16);
  10. the granting by the Authority of approval for the Supplier to commence:
      1. the provision of Operational Services; and/or
      2. Handling Government Data (in Paragraph 15);
  11. the management of changes to the Supplier Information Management System (in Paragraph 17); and
  12. the Authority's additional remedies for breach of this Schedule 5 (*Security Management*), including:
      1. the requirement for Remediation Action Plans (in Paragraph 18);
      2. the appointment of Independent Security Advisers (in Paragraph 19); and
      3. the withholding of Charges by the Authority (in Paragraph 20).

1. Principles of security
   1. The Supplier acknowledges that the Authority places great emphasis on the confidentiality, integrity and availability of the Government Data and, consequently, on the security of:
      1. the Authority System;
      2. the Supplier System;
      3. the Sites;
      4. the Services; and
      5. the Supplier Information Management System.
   2. The Parties shall share information and act in a co‑operative manner at all times to further the principles of security in Paragraph 4.1.
   3. Notwithstanding the involvement of the Authority in the Authority-led Assurance of the Supplier Information Management System, the Supplier remains responsible for:
      1. the security, confidentiality, integrity and availability of the Government Data when that Government Data is under the control of the Supplier or any of its Subcontractors; and
      2. the security of the Supplier Information Management System.
2. Security requirements
   1. The Supplier must, and must ensure that Subcontractors, design, build and manage the Supplier Information Management System in accordance with the Security Management Plan.
   2. The Supplier must, unless otherwise agreed in writing with the Authority:
      1. comply with the Security Requirements in Appendix 1 (*Security Requirements*);
      2. where the relevant option in Paragraph 1 is selected, comply with the Security Requirements for Development in Appendix 2 (*Security Requirements for Development*);
      3. where the relevant option in Paragraph 1 is selected, comply with the Authority Security Policies; and
      4. ensure that Subcontractors comply with:
         1. all Security Requirements in Appendix 1 (*Security Requirements*);
         2. where the relevant option in Paragraph 1 is selected, all Security Requirements for Development in Appendix 2 (*Security Requirements for Development*); and
         3. where the relevant option in Paragraph 1 is selected, all Authority Security Policies,

that apply to the activities that the Subcontractor performs under its Sub‑contract, unless:

* + - 1. Paragraph 5.4 applies; or
      2. the table in Appendix 4 (*Subcontractor Security Requirements and Security Requirements for Development*) limits the Security Requirements or Security Requirements for Development that apply to a Subcontractor.
  1. Where the Authority selects the option in Paragraph 1 requiring the Supplier to comply with the Authority Security Policies, if there is an inconsistency between the Authority Security Requirements and the requirement of this Schedule 5 (*Security Management*), then the requirements of this Schedule 5 (*Security Management*) will prevail to the extent of that inconsistency.
  2. Where a Subcontractor is a SMP Subcontractor, the Supplier shall:
     1. use reasonable endeavours to ensure that the SMP Subcontractor complies with all obligations that this Schedule 5 (*Security Management*) imposes on Subcontractors, including the Security Requirements;
     2. document the differences between those obligations and the obligations that the SMP Subcontractor is prepared to accept in sufficient detail to allow the Authority to form an informed view of the risks concerned; and
     3. take such steps as the Authority may require to mitigate those risks.

1. Authority to proceed
2. Notwithstanding anything in this Contract, the Supplier may not:
   1. commence the provision of any Operational Services; or
   2. Handle any Government Data using the Supplier Information Management System,

unless

* 1. the Supplier has, and ensured that Subcontractors have, obtained the Relevant Certifications under Paragraph 13;
  2. the Supplier has completed an IT Health Check in accordance with Paragraph 12 of the Security Requirements; and
  3. the Authority has issued a Risk Management Approval Statement under Paragraph 15.7.1.

1. Supplier confirmation
   1. The Supplier must, no later than the last day of each Contract Year, provide to the Authority a letter from its [chief executive officer] (or equivalent officer) confirming that, having made due and careful enquiry:
      1. the Supplier has in the previous year carried out all tests and has in place all procedures required in relation to security matters required by this Contract;
      2. subject to Paragraph 7.2:
         1. it has fully complied with all requirements of this Schedule 5 (*Security Management*); and
         2. all Subcontractors have complied with the requirements of this Schedule 5 (*Security Management*) with which the Supplier is required to ensure they comply; and
      3. the Supplier considers that its security and risk mitigation procedures remain effective.
   2. Where the Authority has, in respect of the period covered by the confirmation provided under Paragraph 7.1 agreed in writing that the Supplier need not, or need only partially, comply within any requirement of this Schedule 5 (*Security Management*):
      1. the confirmation must include details of the Authority's agreement; and
      2. confirm that the Supplier has fully complied with that modified requirement.
   3. The Supplier must:
      1. keep and maintain a register setting out all agreements referred to in Paragraph 7.2; and
      2. provide a copy of that register to the Authority on request.
2. Governance, information sharing and co-operation

Governance

* 1. Paragraphs 8.2 to 8.8 apply where a Security Working Group, or Board (as that term is defined in Schedule 17 (*Governance*)), with a similar remit, is not provided for otherwise in this Contract.
  2. The Authority must establish a Security Working Group on which both the Authority and the Supplier are represented.
  3. The notice or other document establishing the Security Working Group must set out:
     1. the Authority members;
     2. the Supplier members;
     3. the chairperson of the Security Working Group;
     4. the date of the first meeting;
     5. the frequency of meetings; and
     6. the location of meetings
  4. The Security Working Group has oversight of all matters relating to the security of the Government Data and the Supplier Information Management System.
  5. The Security Working Group meets:
     1. at least once every 3 months; and
     2. additionally when required by the Authority.
  6. The Supplier must ensure that the Supplier Personnel attending each meeting of the Security Working Group:
     1. have sufficient knowledge and experience to contribute to the discussion of the matters on the agenda for the meeting;
     2. are authorised to make decisions that are binding on the Supplier in respect of those matters, including any decisions that require expenditure or investment by the Supplier; and
     3. where relevant to the matters on the agenda for the meeting, include representatives of relevant Subcontractors.
  7. Any decisions, recommendations or advice of the Security Working Group:
     1. are binding on the Supplier, unless
        1. the Authority agrees otherwise; or
        2. the decision, recommendation or advice of the Security Working Group imposes on the Supplier more onerous requirements than those provided for in this Schedule 5 (*Security Management*); and
     2. do not limit or modify the Supplier's responsibilities under this Schedule 5 (*Security Management*).
  8. Appendix 3 (*Security Working Group*) applies to the Security Working Group.

1. Personnel
   1. The Supplier must ensure that at all times it maintains within the Supplier Personnel sufficient numbers of qualified, skilled security professionals to ensure the Supplier complies with the requirements of this Schedule 5 (*Security Management*).
   2. The Supplier must appoint:
      1. a senior individual within its organisation with accountability for managing security risks and the Supplier's implementation of the requirements of this Schedule 5 (*Security Management*); and
      2. a senior individual within the team responsible for the delivery of the Services with responsibility for managing the security risks to the Supplier Information Management System.
   3. The individuals appointed under Paragraph 9.2:
      1. must have sufficient experience, knowledge and authority to undertake their roles effectively; and
      2. are to be designated as Key Personnel and treated for the purposes of this Contract as Key Personnel, whether or not they are otherwise designated as such.
   4. The Supplier must review, and if necessary replace, the individuals appointed under Paragraph 9.2 if required to do so by the Authority.
   5. To facilitate:
      1. the Authority-led Assurance and oversight of the Supplier Information Management System; and
      2. the Supplier's design, implementation, operation, management and continual improvement of the Security Management Plan and the security of the Services and Supplier Information Management System and otherwise,

at reasonable times and on reasonable notice:

* + 1. the Supplier shall provide access to the Supplier Personnel responsible for information assurance; and
    2. the Authority shall provide access to its personnel responsible for information assurance.

1. Subcontractors
   1. Paragraphs 10.2 to 10.4 are subject to Paragraph 5.4.

SIMS Subcontractor

* 1. A SIMS Subcontractor shall be treated for all purposes as a Key Subcontractor.
  2. In addition to the obligations imposed by this Contract on Key Subcontractors, the Supplier must ensure that the Key Subcontract with each SIMS Subcontractor:
     1. contains obligations no less onerous on the Key Subcontractor than those imposed on the Supplier under this Schedule 5 (*Security Management*); and
     2. provides for the Authority to perform Authority-led Assurance of any part of the Supplier Information Management System that the SIMS Subcontractor provides or operates.

Subcontractors

* 1. The Supplier must, before entering into a binding Sub‑contract with any Subcontractor:
     1. undertake sufficient due diligence of the proposed Subcontractor to provide reasonable assurance that the proposed Subcontractor can perform the obligations that this Schedule 5 (*Security Management*) requires the Supplier ensure that the proposed Subcontractor performs;
     2. keeps adequate records of the due diligence it has undertaken in respect of the proposed Subcontractors; and
     3. provides those records to the Authority on request.

Key Sub‑contractor Default

* 1. Where the Supplier becomes aware of an actual or suspected failure by a Key Sub‑contractor to comply with any obligation in this Schedule 5 (*Security Management*) with which the Supplier is, by virtue of Paragraph 5.2.4, required to ensure the Key Sub‑contractor complies ("**Key Sub‑contractor Default**"), the Supplier must:
     1. as soon as reasonably practicable and in any event within two Working days of becoming aware of the Key Sub‑contractor Default notify the Authority setting out the actual or anticipated effect of the Key Sub‑contractor Default; and
     2. unless the Authority waives the requirement, comply with the Remediation Action Plan process in Paragraph 18.

1. Supplier Information Management System
   1. The Authority must determine:
      1. the scope and component parts of the Supplier Information Management System; and
      2. the boundary between the Supplier Information Management System and the Wider Information Management System.
   2. To enable the Authority to make that determination, the Supplier shall provide the Authority with such documentation and information that the Authority may require regarding the Wider Information Management System.
   3. The Authority shall notify the Supplier, as soon as reasonably practical, following the receipt of such documentation and information, of its decision regarding:
      1. the scope and component parts of the Supplier Information Management System; and
      2. its boundary with the Wider Information Management System.
   4. Before reaching its decision under Paragraph 11.3, the Authority must consult with the Supplier concerning its proposed decision.
   5. The Supplier shall reproduce the Authority's decision as a diagram documenting the components and systems forming part of, and the boundary between, the Supplier Information Management System and the Wider Information Management System.
   6. The diagram prepared under Paragraph 11.3 forms part of the Security Management Plan.
   7. Any proposed change to:
      1. the component parts of the Supplier Information Management System; or
      2. the boundary between the Supplier Information Management System and the Wider Information Management System,

is:

* + 1. an Operational Change to which the Change Control Procedure applies; and
    2. requires approval by the Authority under Paragraph 17; and
    3. the Authority may require the appointment of an Independent Security Adviser to advise on the proposed change.

1. Government Data Handled using Supplier Information Management System
   1. The Supplier acknowledges that the Supplier Information Management System:
      1. is intended only for the Handling of Government Data that is classified as OFFICIAL; and
      2. is not intended for the Handling of Government Data that is classified as SECRET or TOP SECRET,
   2. in each case using the Government Security Classification Policy.
   3. The Supplier must:
      1. not alter the classification of any Government Data; and
      2. if it becomes aware that any Government Data classified as SECRET or TOP SECRET is being Handled using the Supplier Information Management System:
         1. immediately inform the Authority; and
         2. follow any instructions from the Authority concerning that Government Data.
   4. The Supplier must, and must ensure that Subcontractors and Supplier Personnel, when Handling Government Data, comply with:
      1. the Expected Behaviours; and
      2. the Security Controls.
   5. Where there is a conflict between the Expected Behaviours or the Security Controls and this Schedule 5 (*Security Management*) the provisions of this Schedule 5 (*Security Management*) shall apply to the extent of any conflict.
2. Certification Requirements
   1. The Supplier shall ensure that, unless otherwise agreed by the Authority, both:
      1. it; and
      2. any SIMS Subcontractor, any Key Sub-contractor, any Higher-risk Subcontractor and any Medium-risk Subcontractor,

are certified as compliant with the Relevant Certifications, that is to say:

* + 1. in the case of the Supplier, any SIMS Subcontractor and any Key Sub‑contractor:
       1. either:
          1. an ISO Certification in respect of the Supplier Information Management System; or
          2. where the Supplier Information Management System is included within the scope of a wider ISO Certification, that ISO Certification; and
       2. Cyber Essentials Plus;
       3. (or equivalent); and
    2. in the case of any Higher-risk Subcontractor, either:
       1. an ISO Certification in respect of that part of the Supplier Information Management System provided by the Higher-risk Subcontractor;
       2. where that part of the Supplier Information Management System provided by the Higher-risk Subcontractor is included within the scope of a wider ISO Certification, that ISO Certification; or
       3. Cyber Essentials Plus; and
    3. in the case of any Medium-risk Subcontractor, Cyber Essentials (or equivalent).
  1. Unless otherwise agreed by the Authority, before it begins to provide the Services, the Supplier must provide the Authority with a copy of:
     1. the Relevant Certifications for it and any Subcontractor; and
     2. the relevant scope and statement of applicability required under the ISO/IEC 27001 Relevant Certifications.
  2. The Supplier must ensure that at the time it begins to provide the Services, the Relevant Certifications for it and any Subcontractor are:
     1. currently in effect;
     2. together, cover at least the full scope of the Supplier Information Management System; and
     3. are not subject to any condition that may impact the provision of the Services or the Development Activity ("**Certification Requirements**").
  3. The Supplier must notify the Authority promptly, and in any event within 3 Working Days, after becoming aware that, in respect of it or any Subcontractor:
     1. a Relevant Certification in respect of the Supplier Information Management System has been revoked or cancelled by the body that awarded it;
     2. a Relevant Certification in respect of the Supplier Information Management System has expired and has not been renewed by the Supplier;
     3. the Relevant Certifications, together, no longer apply to the full scope of the Supplier Information Management System; or
     4. the body that awarded a Relevant Certification has made it subject to conditions, the compliance with which may impact the provision of the Services (each a "**Certification Default**")
  4. Where the Supplier has notified the Authority of a Certification Default under Paragraph 13.5:
     1. the Supplier must, within 10 Working Days of the date in which the Supplier provided notice under Paragraph 13.5 (or such other period as the Parties may agree) provide a draft plan ("**Certification Rectification Plan"**) to the Authority setting out:
        1. full details of the Certification Default, including a root cause analysis;
        2. the actual and anticipated effects of the Certification Default; and
        3. the steps the Supplier and any Subcontractor to which the Certification Default relates will take to remedy the Certification Default;
     2. the Authority must notify the Supplier as soon as reasonably practicable whether it accepts or rejects the Certification Rectification Plan; and
     3. if the Authority rejects the Certification Rectification Plan, the Supplier must within 5 Working Days of the date of the rejection submit a revised Certification Rectification Plan and Paragraph 13.5.2 will apply to the re‑submitted plan;
     4. the rejection by the Authority of a revised Certification Rectification Plan is a material Default of this Contract; and
     5. if the Authority accepts the Certification Rectification Plan, the Supplier must start work immediately on the plan.

1. Security Management Plan

Purpose of Security Management Plan

* 1. The Authority may, at any time, provide the Supplier with a Statement of Information Risk Appetite.
  2. The Supplier must document in the Security Management Plan how the Supplier and its Subcontractors will:
     1. comply with the requirements set out in this Schedule 5 (*Security Management*) and the Contract in order to ensure the security of the Government Data and the Supplier Information Management System; and
     2. ensure that the operation of the Supplier Information Management System and the provision of the Services does not give rise to any information security risks greater than those set out in that Statement of Information Risk Appetite (where one has been provided).
  3. The Supplier must ensure that:
     1. the Security Management Plan accurately represents the Supplier Information Management System;
     2. the Supplier Information Management System will meet the requirements of this Schedule 5 (*Security Management*) and the Statement of Information Risk Appetite (where one has been provided); and
     3. the residual risks of the Supplier Information Management System are no greater than those provided for in the Statement of Information Risk Appetite (where one has been provided).

Preparation of Security Management Plan

* 1. The Supplier must prepare and submit the Security Management Plan to the Authority:
     1. by the date specified in the Detailed Implementation Plan; or
     2. if no such date is specified, in sufficient time to allow for the Authority to:
        1. approve the Security Management Plan; and
        2. undertake any Authority-led Assurance activity,

before the first Operational Service Commencement Date.

* 1. If Paragraph 14.4.2 applies, and any delay resulting from the Authority-led Assurance causes or contributes to Supplier Non-Performance under Clause 29.1 that delay is not an Authority Cause and the Supplier shall not be entitled to any relief or compensation under Clause 29.

Contents of Security Management Plan

* 1. The Security Management Plan must include:
     1. a formal information risk assessment of, and a risk treatment plan for, the Supplier Information Management System;
     2. a completed statement of applicability under the relevant ISO Certification for the Supplier Information Management System;
     3. the process for managing any security risks from Subcontractors and third parties with access to the Services, the Supplier Information Management System or the Government Data;
     4. unless the Authority has waived this requirement by selecting the relevant option in Paragraph 1, an assessment of the Supplier Information Management System against the table in Appendix 5 (*Secure by Design Principles Evaluation Table*);
     5. unless such requirement is waived by the Authority, the controls the Supplier will implement in respect of the Services and all processes associated with the delivery of the Services, including:
        1. the Supplier System;
        2. the Sites; and
        3. the Authority System (to the extent that it is under the control of the Supplier); and
        4. any IT, Information and data (including the Confidential Information of the Authority and the Government Data) to the extent used by the Authority or the Supplier:
           1. in connection with this Contract or
           2. in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Services;
     6. the Required Changes Register;
     7. evidence that the Supplier and each Subcontractor (so far as those requirements apply) is compliant with:
        1. the Certification Requirements;
        2. the Security Requirements; and
        3. where the relevant option in Paragraph 1 is selected, the Security Requirements for Development;
     8. the diagram documenting the Supplier Information Management System, the Wider Information Management System and the boundary between them (created under Paragraph 11);
     9. an assessment of the Supplier Information Management System against the requirements of this Schedule 5 (*Security Management*), including the Security Requirements and, where the relevant option in Paragraph 1 is selected, the Security Requirements for Development (where applicable);
     10. the process the Supplier will implement immediately after it becomes aware of a Breach of Security to restore normal operations as quickly as possible, minimising any adverse impact on the Government Data, the Authority, the Services and/or users of the Services; and
     11. the following information, so far as is applicable, in respect of each Subcontractor:
         1. the Subcontractor's:
            1. legal name;
            2. trading name (if any); and
            3. registration details (where the Subcontractor is not an individual);
         2. the Relevant Certifications held by the Subcontractor;
         3. the Sites used by the Subcontractor;
         4. the Services provided, or contributed to, by the Subcontractor;
         5. the access the Subcontractor has to the Supplier Information Management System;
         6. the Government Data Handled by the Subcontractor;
         7. the Handling that the Subcontractor will undertake in respect of the Government Data; and
         8. the measures the Subcontractor has in place to comply with the requirements of this Schedule 5 (*Security Management*); and
         9. the due diligence the Supplier has taken to assess that compliance;
     12. the Register of Sites, Support Locations and Third-party Tools;
     13. the Modules Register;
     14. the Support Register;
     15. the Backup and Recovery Plan;
     16. the Remote Working Policy (where the Supplier or a Subcontractor proposes to allow Supplier Personnel to work from a Remote Location); and
     17. details of the protective monitoring that the Supplier will undertake in accordance with Paragraph 14 of the Security Requirements, including:
         1. the additional audit and monitoring the Supplier will undertake of the Supplier Information Management System; and
         2. the retention periods for audit records and event logs.

1. Authority-led Assurance of Supplier Information Management System
   1. The Authority will undertake Authority-led Assurance of the Supplier Information Management System in accordance with this Paragraph 15.
   2. The Supplier acknowledges that the purpose of Authority-led Assurance is to ensure that:
      1. the Security Management Plan accurately represents the Supplier Information Management System;
      2. the Authority has sufficient confidence that the Supplier Information Management System will meet the requirements of this Schedule 5 (*Security Management*) and the Statement of Information Risk Appetite (where one has been provided); and
      3. the residual risks of the Supplier Information Management System are no greater than those provided for in the Statement of Information Risk Appetite (where one has been provided).
   3. The Authority, or representatives appointed by the Authority, will perform Authority-led Assurance.
   4. In addition to any obligations imposed by Schedule 9 (*Implementation Plan*) or Schedule 10 (*Testing Procedures*) the Supplier must ensure that its Detailed Implementation Plan includes:
      1. sufficient information concerning the steps it will take to ensure compliance with the requirements of this Schedule 5 (*Security Management*), including any requirements imposed on Subcontractors;
      2. provision for sufficient time for the Authority to undertake any Authority-led Assurance activities; and
      3. provision for sufficient time for the Supplier to address any issued raised by the Authority should it issue a Risk Management Rejection Notice.
   5. In particular, the Detailed Implementation Plan must include:
      1. the dates on which each subsequent iteration of the Security Management Plan will be delivered to the Authority for review and staged approval; and
      2. the date by which the Supplier is required to have received a Residual Risk Statement from the Authority together with details of each:
         1. tasks the Supplier must complete, including any required Security Tests;
         2. Milestones which must be Achieved; and
         3. Authority Responsibilities which must be completed
            1. for the Supplier to receive a Risk Management Approval Statement pursuant to Paragraph 15.7.1;
   6. To facilitate Authority-led Assurance of the Supplier Information Management System, the Supplier shall provide the Authority and its authorised representatives with:
      1. such access as the Authority or its authorised representative requires to the Supplier Information Management System; and
      2. such other information and/or documentation that the Authority or its authorised representatives may require.
   7. The Authority shall, by the relevant date set out in the Detailed Implementation Plan, review the Security Management Plan and undertake such further investigations as it considers necessary or desirable, and issue to the Supplier:
      1. where satisfied that the:
         1. identified risks to the Supplier Information Management System are adequately and appropriately addressed; and
         2. that the residual risks are:
            1. either:

where the Authority has provided a Statement of Information Risk Appetite, reduced to the level anticipated by that statement; or

where the Authority has not provided a Statement of Information Risk Appetite, reduced to an acceptable level;

* + - * 1. understood and accepted by the Authority; and
        2. recorded in the Residual Risk Statement,

a Risk Management Approval Statement; or

* + 1. where the Authority reasonably considers that:
       1. the identified risks to the Supplier Information Management System have not been adequately or appropriately addressed; or
       2. the residual risks to the Supplier Information Management System have not been reduced:
          1. where the Authority has Provided a Statement of Information Risk Appetite, to the level anticipated by that statement; or
          2. where the Authority has not Provided a Statement of Information Risk Appetite, to an acceptable level,

a Risk Management Rejection Notice, with the reasons for its decision.

* 1. When issued, the Risk Management Approval Statement forms part of the Security Management Plan.
  2. If the Authority issues a Risk Management Rejection Notice, the Supplier shall, within [20] Working Days of the date of the Risk Management Rejection Notice:
     1. address all of the issues raised by the Authority;
     2. update the Security Management Plan; and
     3. notify the Authority that the Supplier Information Management System is ready for re-assessment under Paragraph 15.7.
  3. The process set out in Paragraphs 15.7 to 15.9 shall be repeated until such time as the Authority issues a Risk Management Approval Statement to the Supplier or terminates this Contract.
  4. The Supplier shall not use the Supplier Information Management System to Handle Government Data before receiving a Risk Management Approval Statement.
  5. The Supplier is solely responsible for the costs of:
     1. developing and updating the Security Management Plan; and
     2. implementing changes to the Supplier Information Management System required by any Risk Management Rejection Notice.

1. Monitoring and updating Security Management Plan

Updating Security Management Plan

* 1. The Supplier shall regularly review and update the Security Management Plan, and provide such to the Authority, at least once each year and as required by this Paragraph.

Monitoring

* 1. The Supplier, where it plans to undertake, or after becoming aware of, any of the following:
     1. a significant change to the components or architecture of the Supplier Information Management System;
     2. a significant change in the boundary between the Supplier Information Management System and the Wider Information Management System
     3. a significant change in the operation of the Supplier Information Management System;
     4. the replacement of an existing, or the appointment of a new:
        1. SIMS Subcontractor; or
        2. Subcontractor that Handles Government Data;
     5. a significant change in the quantity of Personal Data held within the Service; and/or
     6. where the Supplier or a Subcontractor has previously Handled Government Data that is Personal Data, other than Special Category Personal Data, it proposes to start to Handle Government Data that is Special Category Personal Data under this Contract;

must:

* + 1. within 2 Working Days notify the Authority; and
    2. within 10 Working Days, or such other timescale as may be agreed with the Authority:
       1. update the Required Changes Register and any other affected parts of the Security Management Plan; and
       2. provide the Authority with a copy those documents for review and approval.
  1. Paragraph 15.2 applies in addition to, and not in substitution of, the Parties obligations to comply with the Change Control Procedure for any Contract Change or Operational Change.
  2. Any proposed change under Paragraph 16.2.1, 16.2.2 or 16.2.6 constitutes a Contract Change to which the Change Control Procedure applies.

1. Review and approval of updated Security Management Plan
   1. Where the Supplier has updated the Security Management Plan under Paragraph 15, the Authority may review the updated plans, require the provision of such further information, and undertake such further investigations as the Authority considers necessary or desirable.
   2. At the conclusion of that review, it may issue to the Supplier:
      1. where satisfied that the:
         1. identified risks to the Supplier Information Management System are adequately and appropriately addressed; and
         2. that the residual risks are:
            1. either:

where the Authority has provided a Statement of Information Risk Appetite, reduced to the level anticipated by that statement; or

where the Authority has not provided a Statement of Information Risk Appetite, reduced to an acceptable level;

* + - * 1. understood and accepted by the Authority; and
        2. recorded in the Residual Risk Statement;

a Risk Management Approval Statement; or

* + 1. where the Authority reasonably considers that:
       1. the identified risks to the Supplier Information Management System have not been adequately or appropriately addressed; or
       2. the residual risks to the Supplier Information Management System have not been reduced:
          1. where the Authority has Provided a Statement of Information Risk Appetite, to the level anticipated by that statement; or
          2. where the Authority has not Provided a Statement of Information Risk Appetite, to an acceptable level,

a Risk Management Rejection Notice, with the reasons for its decision.

1. Changes to the Supplier Information Management System
   1. Notwithstanding anything in this Contract, the Supplier must obtain the approval of the Authority before making any of the following changes to the Supplier Information Management System:
      1. a significant change in the systems or components making up the Supplier Information Management System;
      2. a significant change in the operation or management of the Supplier Information Management System; or
      3. the appointment of a new, or the replacement of an existing:
         1. SIMS Subcontractor; or
         2. Subcontractor that Handles Government Data.
   2. In seeking the Authority's approval to a proposed changes to the Supplier Information Management System, the Supplier must:
      1. update the Required Changes Register;
      2. prepare a proposal for the Authority setting out:
         1. details of the proposed changes to the Supplier Information Management System;
         2. an assessment of the security implications of the proposed change;
         3. a risk assessment of the proposed change; and
         4. any proposed changes to the Security Management Plan; and
      3. provide that paper to the Authority no later than 30 Working Days before the date on which it will consider the proposed changes.
   3. The Authority:
      1. may request such further information as the Authority considers necessary or desirable;
      2. must provide its decision within 20 Working Days of the later of:
         1. the date on which it receives the proposal; or
         2. the date on which it receives any requested further information; and
      3. must not:
         1. unreasonably refuse any proposal by the Supplier; and
         2. must not make any approval subject to unreasonable conditions.
   4. If the Authority does not provide a decision within the period specified in Paragraph 18.3.2, the proposal shall be deemed to have been accepted.

Implementation of changes

* 1. Where the Supplier implements a necessary change to the Supplier Information Management System to address a security related risk or vulnerability, the Supplier shall effect such change at its own cost and expense.
  2. If the Supplier does not implement a necessary change to the Supplier Information Management System to address a security related risk or vulnerability by the date set out in the Required Changes Register:
     1. that failure is a material Default; and
     2. the Supplier shall:
        1. immediately cease using the Supplier Information Management System to Handle Government Data either:
           1. until the Default is remedied, or
           2. unless directed otherwise by the Authority in writing and then only in accordance with the Authority's written directions; and
        2. where such material Default is capable of remedy, remedy such material Default within the timescales set by the Authority (considering the security risks the material Default presents to the Services and/or the Supplier Information Management System).

1. Remediation Action Plan

Preparation of Remediation Action Plan

* 1. This Paragraph 18 applies when:
     1. Key Sub‑contractor Default occurs;
     2. the Authority issues a Risk Management Rejection Notice; or
     3. the Supplier receives a Security Test report identifies vulnerabilities in, or makes findings in respect of, the Supplier Information Management System,

(each a "**RAP Trigger"**).

* 1. The Supplier must within [20] Working Days of the occurrence of a RAP Trigger prepare and submit for approval to the Authority a draft plan ("**Remediation Action Plan"**).
  2. The draft Remediation Action Plan must, in respect of each issue raised by the RAP Trigger, set out:
     1. full details of that issue;
     2. the actual or anticipated effect of that issue;
     3. how the issue will be remedied;
     4. the date by which the issue will be remedied; and
     5. the tests that the Supplier proposes to perform to confirm that the issue has been remedied.

Consideration of Remediation Action Plan

* 1. The Supplier shall promptly provide the Authority with such technical and other information relating to the Supplier Information Management System, Security Management Plan, the IT Health Check report (where applicable), the Key Sub‑contractor (as applicable) or the draft Remediation Action Plan as the Authority requests.
  2. The Authority may:
     1. reject the draft Remediation Action Plan where it considers that the draft Remediation Action Plan is inadequate, providing its reasons for doing so, in which case:
        1. the Supplier shall within [10] Working Days of the date on which the Authority rejected the draft Remediation Action Plan submit a revised draft Remediation Action Plan that takes into account the Authority's reasons; and
        2. Paragraph 12.15 to 12.17 of the Security Requirements shall apply, with appropriate modifications, to the revised draft Remediation Action Plan;
     2. accept the draft Remediation Action Plan, in which case the Supplier must immediately start work on implementing the Remediation Action Plan in accordance with Paragraph 12.19 and 12.20 of the Security Requirements.
  3. Where the Authority unreasonably:
     1. delays its approval; or
     2. rejects,
  4. the draft Remediation Action Plan, the Supplier will not be in breach of this Contract to the extent it demonstrates that any breach:
     1. arose directly from the Authority unreasonably withholding or delaying, as appropriate, its approval of the draft Remediation Action Plan; and
     2. would not have occurred had:
        1. the Authority given its approval, or given its approval in a timely manner, to the draft Remediation Action Plan; and
        2. the Supplier had implemented the draft Remediation Action Plan in accordance with its terms.

Implementing an approved Remediation Action Plan

* 1. In implementing the Remediation Action Plan, the Supplier must conduct such further tests on the Supplier Information Management System as are required by the Remediation Action Plan to confirm that the Remediation Action Plan has fully and correctly implemented.
  2. If any such testing identifies a new risk, new threat, vulnerability or exploitation technique with the potential to affect the security of the Supplier Information Management System, the Supplier shall within [2] Working Days of becoming aware of such risk, threat, vulnerability or exploitation technique:
     1. provide the Authority with a full, unedited and unredacted copy of the test report;
     2. implement interim mitigation measures to vulnerabilities in the Information System known to be exploitable where a security patch is not immediately available; and
     3. as far as practicable, remove or disable any extraneous interfaces, services or capabilities not needed for the provision of the Services within the timescales set out in the test report or such other timescales as may be agreed with the Authority.

1. Independent Security Adviser
   1. The Authority may require the appointment of an Independent Security Adviser where:
      1. there is a proposed change to the Supplier Information Management System (see Paragraph 11.5);
      2. the Authority issues two or more Risk Management Rejection Notices (see Paragraphs 15.7 and 17.2; or
      3. either:
         1. a Security Test report identifies more than ten vulnerabilities classified as either critical or high; or
         2. the Authority rejected a revised draft Remediation Action Plan (see Paragraph 12.21 of Appendix 1 (*Security Requirements*)).
   2. Where the Authority requires the appointment of an Independent Security Adviser, the Independent Security Adviser shall be:
      1. a person selected by the Supplier and approved by the Authority; or
      2. where
         1. the Authority does not approve the persons selected by the Supplier; or
         2. the Supplier does not select any person within 10 Working Days of the date of the notice requiring the Independent Security Adviser's appointment,

a person selected by the Authority.

* 1. The terms of the Independent Security Adviser's appointment shall require that person to:
     1. undertake a detailed review, including a full root cause analysis where the Independent Security Adviser considers it appropriate to do so, of the circumstances that led to that person's appointment; and
     2. provide advice and recommendations on:
        1. steps the Supplier can reasonably take to improvement the security of the Supplier Information Management System; and
        2. where relevant, how the Supplier may mitigate the effects of, and remedy, those and to avoid the occurrence of similar circumstances to those leading to the appointment of the Independent Security Adviser in the future.
  2. The Supplier must permit, and must ensure that relevant Subcontractors permit, the Independent Security Adviser to:
     1. observe the conduct of and work alongside the Supplier Personnel to the extent that the Independent Security Adviser considers reasonable and proportionate having regard to reason for their appointment;
     2. gather any information the Independent Security Adviser considers relevant in the furtherance of their appointment;
     3. write reports and provide information to the Authority in connection with the steps being taken by the Supplier to remedy the matters leading to the Independent Security Adviser's appointment;
     4. make recommendations to the Authority and/or the Supplier as to how the matters leading to their appointment might be mitigated or avoided in the future; and/or
     5. take any other steps that the Authority and/or the Independent Security Adviser reasonably considers necessary or expedient in order to mitigate or rectify matters leading to the Independent Security Adviser's appointment.
  3. The Supplier must, and ensure that relevant Subcontractors:
     1. where relevant, work alongside, provide information to, co‑operate in good faith with and adopt any reasonable methodology in providing the Services recommended by the Independent Security Adviser in order to mitigate or rectify any of the vulnerabilities that led to the appointment of the Independent Security Adviser;
     2. ensure that the Independent Security Adviser has all the access it may require in order to carry out its objective, including access to the Assets;
     3. submit to such monitoring as the Authority and/or the Independent Security Adviser considers reasonable and proportionate in respect of the matters giving rise to their appointment;
     4. implement any recommendations (including additional security measures and/or controls) made by the Independent Security Adviser that have been approved by the Authority within the timescales given by the Independent Security Adviser; and
     5. not terminate the appointment of the Independent Security Adviser without the prior consent of the Authority (unless such consent has been unreasonably withheld).
  4. The Supplier shall be responsible for:
     1. the costs of appointing, and the fees charged by, the Independent Security Adviser; and
     2. its own costs in connection with any action required by the Authority and/or the Independent Security Adviser.
  5. If the Supplier or any relevant Subcontractor:
     1. fails to perform any of the steps required by the Authority in the notice appointing the Independent Security Adviser; and/or
     2. is in Default of any of its obligations under this Paragraph 19,

this is a material Default that is not capable of remedy.

1. Withholding of Charges
   1. The Authority may withhold some or all of the Charges in accordance with the provisions of this Paragraph 20 where:
      1. the Supplier in in material Default of any of its obligations under this Schedule 5 (*Security Management*); or
      2. any of the following matters occurs (where the those matters arise from a Default by the Supplier of its obligations under this this Schedule 5 (*Security Management*)):
         1. a Notifiable Default;
         2. an Intervention Cause; or
         3. a Step‑in Trigger Event.
   2. The Authority may withhold an amount of the Charges that it considers sufficient, in its sole discretion, to incentivise the Supplier to perform the obligations it has Defaulted upon.
   3. Before withholding any Charges under Paragraph 20.1 the Authority must
      1. provide written notice to the Supplier setting out:
         1. the Default in respect of which the Authority has decided to withhold some or all of the Charges;
         2. the amount of the Charges that the Authority will withhold;
         3. the steps the Supplier must take to remedy the Default;
         4. the date by which the Supplier must remedy the Default;
         5. the invoice in respect of which the Authority will withhold the Charges; and
      2. consider any representations that the Supplier may make concerning the Authority's decision.
   4. Where the Supplier does not remedy the Default by the date specified in the notice given under Paragraph 21.3.1, the Authority may retain the withheld amount.
   5. The Supplier acknowledges:
      1. the legitimate interest that the Authority has in ensuring the security of the Supplier Information Management System and the Government Data and, as a consequence, the performance by the Supplier of its obligations under this Schedule 5 (*Security Management*); and
      2. that any Charges that are retained by the Authority are not out of all proportion to the Authority's legitimate interest, even where:
         1. the Authority has not suffered any Losses as a result of the Supplier's Default; or
         2. the value of the Losses suffered by the Authority as a result of the Supplier's Default is lower than the amount of the Charges retained.
   6. The Supplier may raise a Dispute under the Dispute Resolution Procedure with any decision by the Authority to:
      1. withhold any Charges under Paragraph 20.1; or
      2. retain any Charges under Paragraph 20.4.
   7. Any Dispute raised by the Supplier does not prevent the Authority withholding Charges in respect of:
      1. the decision subject to the Dispute; or
      2. any other matter to which this Paragraph 20 applies.
   8. Where any Dispute raised by the Supplier is resolved wholly or partially in its favour, the Authority must return such sums as are specified in any agreement or other document setting out the resolution of the Dispute.
   9. The Authority's right to withhold or retain any amount under this Paragraph 20 are in addition to any other rights that the Authority may have under this Contract or in Law, including any right to claim damages for Losses it suffers arising from the Default.
2. Access to Authority System
   1. Where the Supplier, a Subcontractor or any of the Supplier Personnel is granted access to the Authority System or to the Authority Equipment, it must comply with and ensure that all such Subcontractors and Supplier Personnel comply with, all rules, policies and guidance provided to it and as updated from time to time concerning the Authority System or the Authority Equipment.
3. Security Requirements
4. Location

Location for Relevant Activities

* 1. Unless otherwise agreed with the Authority, the Supplier must, and ensure that its Subcontractors, at all times:
     1. provide the Services;
     2. undertake any activity supporting or managing:
        1. the Services;
        2. the Supplier Information Management System; or
        3. the Wider Information Management System;
     3. store, access or Handle Government Data;
     4. undertake the Development Activity; and
     5. host the Wider Information Management System, including any Sites
  2. (together, the **Relevant Activities**)
  3. only in or from the geographic areas permitted by the Authority in Paragraph 1.
  4. Where the Authority has not selected an option concerning location in Paragraph 1, the Supplier may only undertake the Relevant Activities in or from:
     1. the United Kingdom; or
     2. a territory permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State).
  5. The Supplier must, and must ensure that its Subcontractors, undertake the Relevant Activities in a facility operated by an entity where:
     1. the entity has entered into a binding agreement with the Supplier or Subcontractor (as applicable);
     2. that binding agreement includes obligations on the entity in relation to security management equivalent to those imposed on Subcontractors in this Schedule 5 (*Security Management*);
     3. the Supplier or Subcontractor has taken reasonable steps to assure itself that the entity complies with the binding agreement;
     4. the Supplier has provided the Authority with such information as the Authority requires concerning:
        1. the entity;
        2. the arrangements with the entity; and
        3. the entity's compliance with the binding agreement; and
     5. the Authority has not given the Supplier a Prohibition Notice under Paragraph 1.11.
  6. Where the Supplier cannot comply with one or more of the requirements of Paragraph 1.3:
     1. it must provide the Authority with such information as the Authority requests concerning:
        1. the security controls in places at the relevant location or locations; and
        2. where certain security controls are not, or only partially, implemented the reasons for this;
     2. the Authority may grant approval to use that location or those locations, and that approval may include conditions; and
     3. if the Authority does not grant permission to use that location or those locations, the Supplier must, within such period as the Authority may specify:
        1. cease to store, access or Handle Government Data at that location or those locations;
        2. sanitise, in accordance with instructions from the Authority, such equipment within the information and communications technology system used to store, access or Handle Government Data at that location, or those locations, as the Authority may specify.

Support Locations

* 1. The Supplier must ensure that all Support Locations are located only in the geographic areas permitted by the Authority.
  2. Where the Authority has not selected an option concerning location in Paragraph 1, the Supplier may only locate Support Locations in:
     1. the United Kingdom; or
     2. a territory permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State).
  3. The Supplier must, and must ensure that its Subcontractors operate the Support Locations in a facility operated by an entity where:
     1. the entity has entered into a binding agreement with the Supplier or Subcontractor (as applicable);
     2. the binding agreement includes obligations on the entity in relation to security management equivalent to those relating to Subcontractors in this Schedule 5 (*Security Management*);
     3. the Supplier or Subcontractor has taken reasonable steps to assure itself that the entity complies with the binding agreement;
     4. the Supplier has provided the Authority with such information as the Authority requires concerning:
        1. the entity;
        2. the arrangements with the entity; and
        3. the entity's compliance with the binding agreement; and
     5. the Authority has not given the Supplier a Prohibition Notice under Paragraph 1.11.

Third-party Tools

* 1. Before using any Third-party Tool, the Supplier must, and must ensure that its Subcontractors:
     1. perform adequate due diligence to determine whether there are any recognised security vulnerabilities with that Third-party Tool;
     2. the Supplier has provided the Authority with such information as the Authority requires concerning:
        1. the arrangements with the provider of the Third-party Tool; and
        2. the due diligence undertaken by the Supplier or Subcontractor; and
     3. do not use a Third-party Tool in respect of which the Authority has given the Supplier a Prohibition Notice under Paragraph 1.11.
  2. The Supplier must use, and ensure that Subcontractors use, only those Third-party Tools included in the Register of Sites, Support Locations and Third-party Tools.
  3. The Supplier must not, and must not allow Subcontractors to, use:
     1. a Third-party Tool other than for the activity specified for that Third-party Tool in the Register of Sites, Support Locations and Third-party Tools; or
     2. a new Third-party Tool, or replace an existing Third-party Tool, without the permission of the Authority.

Prohibited Activities

* 1. The Authority may by notice in writing at any time give notice to the Supplier that it and its Subcontractors must not:
     1. undertake or permit to be undertaken some or all of the Relevant Activities or operate Support Locations ("**Prohibited Activity**").
        1. in any particular country or group of countries;
        2. in or using facilities operated by any particular entity or group of entities; or
        3. in or using any particular facility or group of facilities, whether operated by the Supplier, a Subcontractor or a third ‑party entity; or
     2. use any specified Third-party Tool,

(a "**Prohibition Notice**").

* 1. Where the Supplier or Subcontractor, on the date of the Prohibition Notice:
     1. undertakes any Prohibited Activities;
     2. operates any Support Locations; or
     3. employs any Third-party Tool,

affected by the notice, the Supplier must, and must procure that Subcontractors, cease to undertake that Prohibited Activity or employ that Third-party Tool within 40 Working Days of the date of the Prohibition Notice.

1. Physical Security
   1. The Supplier must ensure, and must ensure that Subcontractors ensure, that:
      1. all Sites, locations at which Relevant Activities are performed, or Support Locations ("**Secure Locations**") have the necessary physical protective security measures in place to prevent unauthorised access, damage and interference, whether malicious or otherwise, to Government Data;
      2. the operator of the Secure Location has prepared a physical security risk assessment and a site security plan for the Secure Location; and
      3. the physical security risk assessment and site security plan for each Secure Location:
         1. considers whether different areas of the Secure Location require different security measures based on the functions of each area;
         2. adopts a layered approach to physical security;
         3. has sections dealing with the following matters:
            1. the permiter of the Secure Location;
            2. the building fabric;
            3. security guarding;
            4. visitor and people management;
            5. server and communications rooms;
            6. protection of sensitive data;
            7. closed circuit television;
            8. automated access and control systems;
            9. intruder detection; and
            10. security control rooms.
   2. The Supplier must provide the Authority with the physical security risk assessment and site security plan for any Secure Location within 20 Working Days of a request by the Authority.
2. Vetting, Training and Staff Access

Vetting before performing or managing Services

* 1. The Supplier must not engage Supplier Personnel, and must ensure that Subcontractors do not engage Supplier Personnel in:
     1. any activity relating to the provision or management of the Services; or
     2. any activity that allows or requires the Handling of Government Data,

unless:

* + 1. that individual has passed the security checks listed in Paragraph 3.2; or
    2. the Authority has given prior written permission for a named individual to perform a specific role.
  1. For the purposes of Paragraph 3.1, the security checks are:
     1. the checks required for the HMG Baseline Personnel Security Standard (BPSS) to verify:
        1. the individual's identity;
        2. where that individual will work in the United Kingdom, the individual's nationality and immigration status so as to demonstrate that they have a right to work in the United Kingdom;
        3. the individual's previous employment history; and
        4. that the individual has no Relevant Convictions;
     2. national security vetting clearance to the level specified by the Authority for such individuals or such roles as the Authority may specify; or
     3. such other checks for the Supplier Personnel of Subcontractors as the Authority may specify.

Exception for certain Subcontractors

* 1. Where the Supplier considers it cannot ensure that a Subcontractor will undertake the relevant security checks on any Supplier Personnel, it must:
     1. as soon as practicable, and in any event within [20] Working Days of becoming aware of the issue, notify the Authority;
     2. provide such information relating to the Subcontractor, its vetting processes and the roles the affected Supplier Personnel will perform as the Authority reasonably requires; and
     3. comply, at the Supplier's cost, with all directions the Authority may provide concerning the vetting of the affected Supplier Personnel and the management of the Subcontractor.

Annual training

* 1. The Supplier must ensure, and ensure that Subcontractors ensure, that all Supplier Personnel, complete and pass security training at least once every calendar year that covers:
     1. general training concerning security and data handling;
     2. Phishing, including the dangers from ransomware and other malware; and
     3. the Secure by Design Principles.

Staff access

* 1. The Supplier must ensure, and ensure that Subcontractors ensure, that individual Supplier Personnel can access only the Government Data necessary to allow individuals to perform their role and fulfil their responsibilities in the provision of the Services.
  2. The Supplier must ensure, and ensure that Subcontractors ensure, that where individual Supplier Personnel no longer require access to the Government Data or any part of the Government Data, their access to the Government Data or that part of the Government Data is revoked immediately when their requirement to access Government Data ceases.
  3. Where requested by the Authority, the Supplier must remove, and must ensure that Subcontractors remove, an individual Supplier Personnel's access to the Government Data, or part of that Government Data specified by the Authority, as soon as practicable and in any event within 24 hours of the request.

Remote Working

* 1. The Supplier must ensure, and ensure that Subcontractors ensure, that:
     1. unless in writing by the Authority, Privileged Users do not undertake Remote Working; and
     2. where the Authority permits Remote Working by Privileged Users, the Supplier ensures, and ensures that Subcontractors ensure, that such Remote Working takes place only in accordance with any conditions imposed by the Authority.
  2. Where the Supplier or a Subcontractor wishes to permit Supplier Personnel to undertake Remote Working, it must:
     1. prepare and have approved by the Authority the Remote Working Policy in accordance with this Paragraph;
     2. undertake and, where applicable, ensure that any relevant Subcontractors undertake, all steps required by the Remote Working Policy;
     3. ensure that Supplier Personnel undertake Remote Working only in accordance with the Remote Working Policy; and
     4. may not permit any Supplier Personnel of the Supplier or any Subcontractor to undertake Remote Working until the Remote Working Policy is approved by the Authority.
  3. The Remote Working Policy must include or make provision for the following matters:
     1. restricting or prohibiting Supplier Personnel from printing documents in any Remote Location;
     2. restricting or prohibiting Supplier Personnel from downloading any Government Data to any End-user Device other than an End User Device that:
        1. is provided by the Supplier or Subcontractor (as appropriate); and
        2. complies with the requirements set out in Paragraph 4 (*End-user Devices*);
     3. ensuring that Supplier Personnel comply with the Expected Behaviours (so far as they are applicable);
     4. giving effect to the Security Controls (so far as they are applicable);
     5. for each different category of Supplier Personnel subject to the proposed Remote Working Policy:
        1. the types and volumes of Government Data that the Supplier Personnel can Handle in a Remote Location and the Handling that those Supplier Personnel will undertake;
        2. any identified security risks arising from the proposed Handling in a Remote Location;
        3. the mitigations, controls and security measures the Supplier or Subcontractor (as applicable) will implement to mitigate the identified risks;
        4. the residual risk levels following the implementation of those mitigations, controls and measures;
        5. when the Supplier or Subcontractor (as applicable) will implement the proposed mitigations, controls and measures; and
        6. the business rules with which the Supplier Personnel must comply; and
     6. how the Supplier or the Subcontractor (as applicable) will:
        1. communicate the Remote Working Policy and business rules to Supplier Personnel; and
        2. enforce the Remote Working Plan and business rules.
  4. The Supplier may submit a proposed Remote Working Policy to the Authority for consideration at any time.
  5. The Authority must, within 20 Working Days of the submission of a proposed Remote Working Plan, either:
     1. approve the proposed Remote Working Policy, in which case the Supplier must, and ensure that any applicable Subcontractor, implements the approved Remote Working Plan in accordance with its terms; or
     2. reject the proposed Remote Working Policy, in which case:
        1. the Authority may set out any changes to the proposed Remote Working Policy the Authority requires to make the plan capable of approval; and
        2. the Supplier may:
           1. revise the proposed Remote Working Plan; and
           2. re-submit the proposed Remote Working Plan to the Authority for approval under Paragraph 3.11.

1. End-user Devices
   1. The Supplier must manage, and must ensure that all Subcontractors manage, all End‑user Devices on which Government Data or Code is stored or Handled in accordance the following requirements:
      1. the operating system and any applications that store, Handle or have access to Government Data or Code must be in current support by the vendor, or the relevant community in the case of open source operating systems or applications;
      2. users must authenticate before gaining access;
      3. all Government Data and Code must be encrypted using an encryption tool agreed to by the Authority;
      4. the End-user Device must lock and require any user to re‑authenticate after a period of time that is proportionate to the risk environment, during which the End-user Device is inactive;
      5. the End-user Device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Government Data and Code to ensure the security of that Government Data and Code;
      6. the Suppler or Subcontractor, as applicable, can, without physical access to the End-user Device, remove or make inaccessible all Government Data or Code stored on the device and prevent any user or group of users from accessing the device; and
      7. all End-user Devices are within the scope of any Relevant Certification.
   2. The Supplier must comply, and ensure that all Subcontractors comply, with the recommendations in NCSC Device Guidance as if those recommendations were incorporated as specific obligations under this Contract.
   3. Where there is any conflict between the requirements of this Schedule 5 (*Security Management*) and the requirements of the NCSC Device Guidance, the requirements of this Schedule 5 (*Security Management*) take precedence.
2. Hardware and software support
   1. Before using any software as part of the Supplier Information Management System, the Supplier must:
      1. perform adequate due diligence to determine whether there are any recognised security vulnerabilities with that software; and
      2. where there are any recognised security vulnerabilities, either:
         1. remedy vulnerabilities; or
         2. ensure that the design of the Supplier Information Management System mitigates those vulnerabilities.
   2. The Supplier must ensure that all software used to provide the Services remains at all times in full security support, including any extended or bespoke security support.
   3. The Supplier must produce and maintain a register of all software that forms the Supplier Information Management System ("**Support Register**").
   4. The Support Register must include in respect of each item of software:
      1. any vulnerabilities identified with the software and the steps the Supplier has taken to remedy or mitigate those vulnerabilities;
      2. the date, so far as it is known, that the item will cease to be in mainstream security support; and
      3. the Supplier's plans to upgrade the item before it ceases to be in mainstream security support.
   5. The Supplier must:
      1. review and update the Support Register:
         1. within 10 Working days of becoming aware of any new vulnerability in any item of software;
         2. within 10 Working Days of becoming aware of the date on which, or any change to the date on which, any item of software will cease to be in mainstream security report;
         3. within 10 Working Days of introducing new software, or removing existing software, from the Supplier Information Management System; and
         4. at least once every 12 months; and
      2. provide the Authority with a copy of the Support Register:
         1. whenever it updates the Support Register; and
         2. otherwise when the Authority requests.
   6. Where any element of the Supplier Information Management System consists of COTS Software, the Supplier shall ensure:
      1. those elements are always in mainstream or extended security support from the relevant vendor; and
      2. the COTS Software is not more than one version or major release behind the latest version of the software.
   7. The Supplier shall ensure that all hardware used to provide the Services, whether used by the Supplier or any Subcontractor is, at all times, remains in mainstream vendor support, that is, that in respect of the hardware, the vendor continues to provide:
      1. regular firmware updates to the hardware; and
      2. a physical repair or replacement service for the hardware.
   8. The Supplier must ensure that where any software or hardware component of the Supplier Information Management System is no longer required to provide the Services or has reached the end of its life it is removed or disconnected from the Supplier Information Management System.
3. Encryption
   1. Before Handling any Government Data, the Supplier must agree with the Authority the encryption methods that it and any Subcontractors that Handle Government Data will use to comply with this Paragraph 6.
   2. Where this Paragraph 6 requires Government Data to be encrypted, the Supplier must use, and ensure that Subcontractors use, the methods agreed by the Authority under Paragraph 6.1.
   3. Unless Paragraph 6.4 applies, the Supplier must ensure, and must ensure that all Subcontractors ensure, that Government Data is encrypted:
      1. when stored at any time when no operation is being performed on it, including when stored on any portable storage media; and
      2. when transmitted.
   4. Where the Supplier, or a Subcontractor, cannot encrypt Government Data as required by Paragraph 6.2, the Supplier must:
      1. immediately inform the Authority of the subset or subsets of Government Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;
      2. provide details of the protective measures the Supplier or Subcontractor (as applicable) proposes to take to provide equivalent protection to the Authority as encryption; and
      3. provide the Authority with such additional information relating to the information provided under sub-Paragraphs (a) and (b) as the Authority may require.
   5. The Authority, the Supplier and, where the Authority requires, any relevant Subcontractor shall meet to agree appropriate protective measures for the unencrypted Government Data.
   6. Where the Authority and Supplier reach agreement, the Supplier must update the Security Management Plan to include:
      1. the subset or subsets of Government Data not encrypted and the circumstances in which that will occur; and
      2. the protective measure that the Supplier and/or Subcontractor will put in place in respect of the unencrypted Government Data.
   7. Where the Authority and Supplier do not reach agreement within 40 Working Days of the date on which the Supplier first notified the Authority that it could not encrypt certain Government Data, either party may refer the matter to [be determined by an expert in accordance with the Dispute Resolution Procedure].
4. Backup and recovery of Government Data

Backups and recovery of Government Data

* 1. The Supplier must backup and recover the Government Data in accordance with the Backup and Recovery Plan to ensure the recovery point objective and recovery time objective in Paragraph 7.3(a).
  2. Any backup system operated by the Supplier or Subcontractor forms part of the Supplier System or that Subcontractor's System to which this Schedule 5 (*Security Management*) and the Security Requirements apply.

Backup and Recovery Plan

* 1. Unless otherwise required by the Authority, the Backup and Recovery Plan must provide for:
     1. in the case of a full or partial failure of the Supplier System or a Subcontractor's System:
        1. a recovery time objective of [**insert period**]; and
        2. a recovery point objective of [**insert period**]; and
     2. a retention period of [**insert period**].
  2. In doing so, the Backup and Recovery Plan must ensure that in respect of any backup system operated by the Supplier or a Subcontractor:
     1. the backup location for Government Data is sufficiently physically and logically separate from the rest of the Supplier System or a Subcontractor's System that it is not affected by any Disaster affecting the rest of the Supplier System or a Subcontractor's System;
     2. there is sufficient storage volume for the amount of Government Data to be backed up;
     3. all back-up media for Government Data is used in accordance with the manufacturer's usage recommendations;
     4. newer backups of Government Data do not overwrite existing backups made during the retention period specified in Paragraph 7.3(a)(ii);
     5. the backup system monitors backups of Government Data to:
        1. identifies any backup failure; and
        2. confirm the integrity of the Government Data backed up;
     6. any backup failure is remedied promptly;
     7. the backup system monitors the recovery of Government Data to:
        1. identify any recovery failure;
        2. confirm the integrity of Government Data recovered; and
     8. any recovery failure is promptly remedied.

1. Email
   1. The Supplier must ensure that where the Supplier Information Management System will provide an Email Service to the Authority, it:
      1. supports transport layer security ("**TLS**") version 1.2, or higher, for sending and receiving emails;
      2. supports TLS Reporting ("**TLS‑RPT**");
      3. is capable of implementing:
         1. domain ‑based message authentication, reporting and conformance ("**DMARC**");
         2. sender policy framework ("**SPF**"); and
         3. domain keys identified mail ("**DKIM**"); and
      4. is capable of complying in all respects with any guidance concerning email security as issued or updated from time to time by:
         1. the UK Government (current version at <https://www.gov.uk/guidance/set-up-government-email-services-securely>; or
         2. the NCSC (current version at <https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing>).
2. DNS
   1. Unless otherwise agreed by the Authority, the Supplier must ensure that the Supplier Information Management System uses the UK public sector Protective DNS ("**PDNS**") service to resolve internet DNS queries.
3. Malicious Software
   1. The Supplier shall install and maintain Anti‑virus Software or procure that Anti‑virus Software is installed and maintained on the Supplier Information Management System.
   2. The Supplier must ensure that such Anti‑virus Software:
      1. prevents the installation of the most common forms of Malicious Software in the Supplier Information Management System and the Development Environment;
      2. is configured to perform automatic software and definition updates;
      3. provides for all updates to be the Anti‑virus Software to be deployed within [10] Working Days of the update's release by the vendor;
      4. performs regular scans of the Supplier Information Management System to check for and prevent the introduction of Malicious Software; and
      5. where Malicious Software has been introduced into the Supplier Information Management System, identifies, contains the spread of, and minimises the impact of Malicious Software.
   3. If Malicious Software is found, the Parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Government Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.
   4. Any Breach of Security caused by Malicious Software where the Breach of Security arose from a failure by the Supplier, or a Subcontractor, to comply with this Paragraph 10 is a material Default.
4. Vulnerabilities
   1. Unless the Authority otherwise agrees, the Supplier must ensure that it or any relevant Subcontractor applies security patches to any vulnerabilities in the Supplier Information Management System no later than:
      1. 7 days after the public release of patches for vulnerabilities classified as "critical";
      2. 30 days after the public release of patches for vulnerabilities classified as "important"; and
      3. 60 days after the public release of patches for vulnerabilities classified as "other".
   2. The Supplier must:
      1. scan the Supplier Information Management System and the Development Environment at least once every month to identify any unpatched vulnerabilities; and
      2. if the scan identifies any unpatched vulnerabilities ensure they are patched in accordance with Paragraph 11.1.
   3. For the purposes of this Paragraph 11, the Supplier must implement a method for classifying vulnerabilities to the Supplier Information Management System as "critical", "important" or "other" that is aligned to recognised vulnerability assessment systems, such as:
      1. the National Vulnerability Database's vulnerability security ratings; or
      2. Microsoft's security bulletin severity rating system.
5. Security testing

Responsibility for security testing

* 1. The Supplier is solely responsible for:
     1. the costs of conducting any security testing required by this Paragraph 12; and
     2. the costs of implementing any findings, or remedying any vulnerabilities, identified in that security testing.

Security tests by Supplier

* 1. The Supplier must:
     1. before submitting the draft Security Management Plan to the Authority for a decision under Paragraph 15 of this Schedule 5 *(Security Management)*;
     2. at least once during each Contract Year; and
     3. when required to do so by the Authority;
     4. undertake the following activities:
        1. conduct security testing of the Supplier Information Management System ("**IT Health Check**") in accordance with Paragraph 12.8 to 12.10; and
        2. implement any findings, and remedy any vulnerabilities identified by the IT Health Check in accordance with Paragraphs 12.11 to 12.21.
  2. In addition to its obligations under Paragraph 12.2, the Supplier must undertake any tests required by:
     1. any Remediation Action Plan;
     2. the ISO27001 Certification Requirements;
     3. the Security Management Plan; and
     4. the Authority, following a Breach of Security or a significant change, as assessed by the Authority, to the components or architecture of the Supplier Information Management System,

(each a Supplier Security Test).

* 1. The Supplier must:
     1. design and implement the Supplier Security Tests so as to minimise the impact on the delivery of the Services;
     2. agree the date, timing, content and conduct of such Supplier Security Tests in advance with the Authority.
  2. Where the Supplier fully complies with Paragraph 12.4, if a Supplier Security Test causes a Performance Failure in a particular Measurement Period, the Supplier shall be entitled to relief in respect of such Performance Failure for that Measurement Period.
  3. The Authority may send a representative to witness the conduct of the Supplier Security Tests.
  4. The Supplier shall provide the Authority with a full, unedited and unredacted copy of the results of such Security Tests (in a form approved by the Authority in advance) as soon as practicable, and in any case within 10 Working Days, after completion of each Supplier Security Test

IT Health Checks

* 1. In arranging an IT Health Check, the Supplier must:
     1. use only a CHECK Service Provider to perform the IT Health Check;
     2. ensure that the CHECK Service Provider uses a qualified CHECK Team Leader and CHECK Team Members to perform the IT Health Check;
     3. design and plan for the IT Health Check so as to minimise the impact of the IT Health Check on the Supplier Information Management System and the delivery of the Services.
     4. promptly provide the Authority with such technical and other information relating to the Information Management System as the Authority requests;
     5. include within the scope of the IT Health Check such tests as the Authority requires; and
     6. agree with the Authority the scope, aim and timing of the IT Health Check.
  2. The Supplier must commission the IT Health Check in accordance with the scope, aim and timing agreed by the Authority.
  3. Following completion of an IT Health Check, the Supplier must provide the Authority with a full, unedited and unredacted copy of the report relating to the IT Health Check without delay and in any event within 10 Working Days of its receipt by the Supplier.

Remedying vulnerabilities

* 1. In addition to complying with Paragraphs 12.13 to 12.21, the Supplier must remedy:
     1. any vulnerabilities classified as critical in a Security Test report within 5 Working Days of becoming aware of the vulnerability and its classification;
     2. any vulnerabilities classified as high in a Security Test report within one month of becoming aware of the vulnerability and its classification; and
     3. any vulnerabilities classified as medium in a Security Test report within 3 months of becoming aware of the vulnerability and its classification.
  2. The Supplier must notify the Authority immediately if it does not, or considers it will not be able to, remedy the vulnerabilities classified as critical, high or medium in a Security Test report within the time periods specified in Paragraph 12.11.

Responding to a Security Test report

* 1. Where the Security Test report identifies vulnerabilities in, or makes findings in respect of, the Supplier Information Management System, the Supplier must within [20] Working Days of receiving the Security Test report, prepare and submit for approval to the Authority a draft plan addressing the vulnerabilities and findings ("**Remediation Action Plan**").
  2. Where the Authority has commissioned a root cause analysis under Paragraph 12.21, the Supplier shall ensure that the draft Remediation Action Plan addresses that analysis.
  3. The draft Remediation Action Plan must, in respect of each vulnerability identified or finding made by the Security Test report:
     1. how the vulnerability or finding will be remedied;
     2. the date by which the vulnerability or finding will be remedied; and
     3. the tests that the Supplier proposes to perform to confirm that the vulnerability has been remedied or the finding addressed.
  4. The Supplier shall promptly provide the Authority with such technical and other information relating to the Supplier Information Management System, the IT Health Check report or the draft Remediation Action Plan as the Authority requests.
  5. The Authority may:
     1. reject the draft Remediation Action Plan where it considers that the draft Remediation Action Plan is inadequate, providing its reasons for doing so, in which case:
        1. the Supplier shall within 10 Working Days of the date on which the Authority rejected the draft Remediation Action Plan submit a revised draft Remediation Action Plan that takes into account the Authority's reasons; and
        2. Paragraph 12.15 to 12.17 shall apply, with appropriate modifications, to the revised draft Remediation Action Plan;
     2. accept the draft Remediation Action Plan, in which case the Supplier must immediately start work on implementing the Remediation Action Plan in accordance with Paragraph 12.19 and 12.20.
  6. Where the Authority unreasonably:
     1. delays its approval; or
     2. rejects,

the draft Remediation Action Plan, the Supplier will not be in breach of this Contract to the extent it demonstrates that any breach:

* + 1. arose directly from the Authority unreasonably withholding or delaying, as appropriate, its approval of the draft Remediation Action Plan; and
    2. would not have occurred had:
       1. the Authority given its approval, or given its approval in a timely manner, to the draft Remediation Action Plan; and
       2. the Supplier had implemented the draft Remediation Action Plan in accordance with its terms.

Implementing an approved Remediation Action Plan

* 1. In implementing the Remediation Action Plan, the Supplier must conduct such further tests on the Supplier Information Management System as are required by the Remediation Action Plan to confirm that the Remediation Action Plan has fully and correctly implemented.
  2. If any such testing identifies a new risk, new threat, vulnerability or exploitation technique with the potential to affect the security of the Supplier Information Management System, the Supplier shall within two Working Days of becoming aware of such risk, threat, vulnerability or exploitation technique:
     1. provide the Authority with a full, unedited and unredacted copy of the test report;
     2. implement interim mitigation measures to vulnerabilities in the Information System known to be exploitable where a security patch is not immediately available;
     3. as far as practicable, remove or disable any extraneous interfaces, services or capabilities not needed for the provision of the Services within the timescales set out in the test report or such other timescales as may be agreed with the Authority.

Significant vulnerabilities

* 1. Where:
     1. a Security Test report identifies more than 10 vulnerabilities classified as either critical or high; or
     2. the Authority rejected a revised draft Remediation Action Plan,

the Authority may, at the Supplier's cost, either:

* + 1. appoint an independent and appropriately qualified and experienced security architect and adviser to perform a root cause analysis of the identified vulnerabilities; or
    2. give notice to the Supplier requiring the appointment as soon as reasonably practicable, and in any event within 10 Working Days, of an Independent Security Adviser.

1. Access Control
   1. The Supplier must, and must ensure that all Subcontractors:
      1. identify and authenticate all persons who access the Supplier Information Management System and Sites before they do so;
      2. require multi‑factor authentication for all user accounts that have access to Government Data or that are Privileged Users;
      3. allow access only to those parts of the Supplier Information Management System and Sites that those persons require; and
      4. maintain records detailing each person's access to the Supplier Information Management System and Sites, and make those records available to the Authority on request.
   2. The Supplier must ensure, and must ensure that all Subcontractors ensure, that the user accounts for Privileged Users of the Supplier Information Management System:
      1. are allocated to a single, individual user;
      2. are accessible only from dedicated End-user Devices;
      3. are configured so that those accounts can only be used for system administration tasks;
      4. require passwords with high complexity that are changed regularly;
      5. automatically log the user out of the Supplier Information Management System after a period of time that is proportionate to the risk environment during which the account is inactive; and
      6. are:
         1. restricted to a single role or small number of roles;
         2. time limited; and
         3. restrict the Privileged User's access to the internet.
   3. The Supplier must ensure, and must ensure that all Subcontractors ensure, that it logs all activity of the Privileged Users while those users access those accounts and keeps the activity logs for 20 Working Days before deletion.
   4. The Supplier must require, and must ensure that all Subcontractors require, that Privileged Users use unique and substantially different high ‑complexity passwords for their different accounts on the Supplier Information Management System.
   5. The Supplier must, and must ensure that all Subcontractors:
      1. configure any hardware that forms part of the Supplier Information Management System that is capable of requiring a password before it is accessed to require a password; and
      2. change the default password of that hardware to a password of high complexity that is substantially different from the password required to access similar hardware.
2. Event logging and protective monitoring

Protective Monitoring System

* 1. The Supplier must, and must ensure that Subcontractors, implement an effective system of monitoring and reports, analysing access to and use of the Supplier Information Management System, the Development Environment, the Government Data and the Code to:
     1. identify and prevent potential Breaches of Security;
     2. respond effectively and in a timely manner to Breaches of Security that do occur;
     3. identify and implement changes to the Supplier Information Management System to prevent future Breaches of Security; and
     4. help detect and prevent any potential criminal offence relating to fraud, bribery or corruption using the Supplier Information Management System,

("**Protective Monitoring System**").

* 1. The Protective Monitoring System must provide for:
     1. event logs and audit records of access to the Supplier Information Management system; and
     2. regular reports and alerts to identify:
        1. changing access trends;
        2. unusual usage patterns; or
        3. the access of greater than usual volumes of Government Data;
     3. the detection and prevention of any attack on the Supplier Information Management System or the Development Environment using common cyber‑attack techniques; and
     4. any other matters required by the Security Management Plan.

Event logs

* 1. The Supplier must ensure that, unless the Authority otherwise agrees, any event logs do not log:
     1. personal data, other than identifiers relating to users; or
     2. sensitive data, such as credentials or security keys.

Provision of information to Authority

* 1. The Supplier must provide the Authority on request with:
     1. full details of the Protective Monitoring System it has implemented; and
     2. copies of monitoring logs and reports prepared as part of the Protective Monitoring System.

Changes to Protective Monitoring System

* 1. The Authority may at any time require the Supplier to update the Protective Monitoring System to:
     1. respond to a specific threat identified by the Authority;
     2. implement additional audit and monitoring requirements; and
     3. stream any specified event logs to the Authority's security information and event management system.

1. Audit rights

Right of audit

* 1. The Authority may undertake an audit of the Supplier or any Subcontractor to:
     1. verify the Supplier's or Subcontractor's (as applicable) compliance with the requirements of this Schedule 5 (*Security Management*) and the Data Protection Laws as they apply to Government Data;
     2. inspect the Supplier Information Management System (or any part of it);
     3. review the integrity, confidentiality and security of the Government Data; and/or
     4. review the integrity and security of the Code.
  2. Any audit undertaken under Paragraph 15.1:
     1. may only take place during the Term and for a period of 18 months afterwards; and
     2. is in addition to any other rights of audit the Authority has under this Contract.
  3. The Authority may not undertake more than one audit under Paragraph 15.1 in each calendar year unless the Authority has reasonable grounds for believing:
     1. the Supplier or any Subcontractor has not complied with its obligations under this Contract or the Data Protection Laws as they apply to the Government Data;
     2. there has been or is likely to be a Breach of Security affecting the Government Data or the Code; or
     3. where vulnerabilities, or potential vulnerabilities, in the Code have been identified by:
        1. an IT Health Check; or
        2. a Breach of Security.

Conduct of audits

* 1. The Authority must use reasonable endeavours to provide 15 Working Days' notice of an audit.
  2. The Authority must when conducting an audit:
     1. comply with all relevant policies and guidelines of the Supplier or Subcontractor (as applicable) concerning access to the Suppler Information Management System the Authority considers reasonable having regard to the purpose of the audit; and
     2. use reasonable endeavours to ensure that the conduct of the audit does not unreasonably disrupt the Supplier or Subcontractor (as applicable) or delay the provision of the Services.
  3. The Supplier must, and must ensure that Subcontractors, on demand provide the Authority with all co‑operation and assistance the Authority may reasonably require, including:
     1. all information requested by the Authority within the scope of the audit;
     2. access to the Supplier Information Management System; and
     3. access to the Supplier Personnel.

Response to audit findings

* 1. Where an audit finds that:
     1. the Supplier or a Subcontractor has not complied with this Contract or the Data Protection Laws as they apply to the Government Data; or
     2. there has been or is likely to be a Security Breach affecting the Government Data,
  2. the Authority may require the Supplier to remedy those defaults at its own cost and expense and within the time reasonably specified by the Authority.
  3. The exercise by the Authority of any rights it may have under this Paragraph 15 does not affect the exercise by it of any other or equivalent rights it may have under this Contract in respect of the audit findings.

1. Breach of Security

Reporting Breach of Security

* 1. If either party becomes aware of a Breach of Security it shall notify the other as soon as reasonably practicable after becoming aware of the breach, and in any event within [24] hours.

Immediate steps

* 1. The Supplier must, upon becoming aware of a Breach of Security immediately take those steps identified in the Security Management Plan and all other steps reasonably necessary to:
     1. minimise the extent of actual or potential harm caused by such Breach of Security;
     2. remedy such Breach of Security to the extent possible;
     3. apply a tested mitigation against any such Breach of Security; and
     4. prevent a further Breach of Security in the future which exploits the same root cause failure;

Subsequent action

* 1. As soon as reasonably practicable and, in any event, within 5 Working Days of the occurrence of the Breach of Security, or such other period specified by the Authority, provide to the Authority:
     1. full details of the Breach of Security; and
     2. if required by the Authority:
        1. a root cause analysis; and
        2. a draft plan addressing the Breach of Security,

(a "**Breach Action Plan**").

* 1. The draft Breach Action Plan must set out:
     1. in respect of each issue identified in the root cause analysis:
        1. how the issue will be remedied;
        2. the date by which the issue will be remedied; and
        3. the tests that the Supplier proposes to perform to confirm that the issue has been remedied or the finding addressed;
     2. the assistance the Supplier will provide to the Authority to resolve any impacts on the Authority, the Government Data and the Code;
     3. the Supplier's communication and engagement activities in respect of the Breach of Security, including any communication or engagement with individuals affected by any Breach of Security that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data; and
     4. the infrastructure, services and systems (including any contact centre facilities) the Supplier will establish to undertake the remediation, communication and engagement activities.
  2. The Supplier shall promptly provide the Authority with such technical and other information relating to the draft Breach Action Plan as the Authority requests.
  3. The Authority may:
     1. reject the draft Breach Action Plan where it considers that the draft Breach Action Plan is inadequate, providing its reasons for doing so, in which case:
        1. the Supplier shall within 10 Working Days of the date on which the Authority rejected the draft Breach Action Plan, or such other period as the Authority requires, submit a revised draft Breach Action Plan that takes into account the Authority's reasons; and
        2. Paragraph 16.5 and 16.6 shall apply to the revised draft Breach Action Plan; or
     2. accept the draft Breach Action Plan, in which case the Supplier must immediately start work on implementing the Breach Action Plan.
  4. When implementing the Breach Action Plan, the Supplier must:
     1. establish infrastructure, services and systems referred to in the Breach Action Plan;
     2. communicate and engage with affected individuals in accordance with the Breach Action Plan;
     3. communicate and engage with the Authority and stakeholders identified by the Authority in accordance with the Breach Plan and as otherwise required by the Authority;
     4. engage and deploy such additional resources as may be required to perform its responsibilities under the Breach Plan and this Contract in respect of the Personal Data Breach without any impact on the provision of the Services; and
     5. continue to implement the Breach Action Plan until the Authority indicates that the Breach of Security and the impacts on the Authority, the Government Data, the Code and the affected individuals have been resolved to the Authority's satisfaction.
  5. The obligation to provide and implement a Breach Action Plan under Paragraphs 16.3 to 16.7 continues notwithstanding the expiry or termination of this Contract.

Costs of preparing and implementing Breach Action Plan

* 1. The Supplier is solely responsible for its costs in preparing and implementing a Breach Action Plan.

Reporting of Breach of Security to regulator

* 1. Where the Law requires the Supplier report a Breach of Security to the appropriate regulator, the Supplier must:
     1. make that report within the time limits:
        1. specified by the relevant regulator; or
        2. otherwise required by Law;
     2. to the extent that the relevant regulator or the Law permits, provide the Authority with a full, unredacted and unedited copy of that report at the same time it is sent to the relevant regulator.
  2. Where the Law requires the Authority to report a Breach of Security to the appropriate regulator, the Supplier must:
     1. provide such information and other input as the Authority requires within the timescales specified by the Authority; and
     2. ensure so far as practicable the report it sends to the relevant regulator is consistent with the report provided by the Authority.

1. **Exit management**
   1. In addition to any obligations on the Supplier under Schedule 21 (*Exit Management*) the Supplier must:
      1. agree with the Authority and, where required by the Supplier, the Replacement Supplier; and
      2. document as part of the Exit Plan,

a plan for the migration of the Government Data to the Authority and/or the Replacement Supplier (as required by the Authority) ("**Data Migration Plan**").

* 1. The Data Migration Plan must, at a minimum, include:
     1. the data formats of the Government Data;
     2. the roles and responsibilities of the Supplier, the Authority and (where applicable) the Replacement Supplier;
     3. the methods to be used to securely transfer the data;
     4. the timescales for the completion of all tasks and activities set out in the Data Migration Plan; and
     5. how data migration will be managed to ensure continuity of Services and the integrity, confidentiality and accessibility of the Government Data during that process.
  2. The Supplier shall comply with the provisions of the Data Migration Plan during Exit Management.

1. **Return and deletion of Government Data**
   1. The Supplier must create and maintain a register of:
      1. all Government Data the Supplier, or any Subcontractor, receives from or creates for the Authority; and
      2. those parts of the Supplier Information Management System, including those parts of the Supplier Information Management System that are operated or controlled by any Subcontractor, on which the Government Data is stored,

("**Government Data Register**").

* 1. The Supplier must:
     1. review and update the Government Data Register:
        1. within 10 Working Days of the Supplier or any Subcontractor changes those parts of the Supplier Information Management System on which the Government Data is stored;
        2. within 10 Working Days of a significant change in the volume, nature or overall sensitivity of the Government Data stored on the Supplier Information Management System;
        3. at least once every 12 months; and
     2. provide the Authority with a copy of the Government Data Register:
        1. whenever it updates the Government Data Register; and
        2. otherwise when the Authority requests.
  2. Subject to Paragraph 18.4, the Supplier must, and must ensure that all Subcontractors, securely erase any or all Government Data held by the Supplier or Subcontractor, including any or all Code:
     1. when requested to do so by the Authority; and
     2. using a deletion method agreed with the Authority that ensures that even a determined expert using specialist techniques can recover only a small fraction of the data deleted.
  3. Paragraph 18.3 does not apply to Government Data:
     1. that is Personal Data in respect of which the Supplier is a Controller;
     2. to which the Supplier has rights to Handle independently from this Contract; or
     3. in respect of which, the Supplier is under an obligation imposed by Law to retain.
  4. The Supplier must, and must ensure that all Subcontractors, provide the Authority with copies of any or all Government Data held by the Supplier or Subcontractor, including any or all Code:
     1. when requested to do so by the Authority; and
     2. using the method specified by the Authority.

1. Security Requirements for Development
2. **Secure Software Development by Design**
   1. The Supplier must, and must ensure that all Subcontractors engaged in Development Activity, implement secure development and deployment practices to ensure that:
      1. no Malicious Software is introduced into the Developed System or the Supplier Information Management System.
      2. the Developed System can continue to function in accordance with the Specification:
         1. in unforeseen circumstances; and
         2. notwithstanding any attack on the Developed System using common cyber‑attack techniques, including attacks using those vulnerabilities identified at any time in the OWASP Top Ten.
   2. To those ends, the Supplier must, and ensure that all Subcontractors engaged in Development Activity:
      1. comply with the Secure Development Guidance as if its requirements were terms of this Contract; and
      2. document the steps taken to comply with that guidance as part of the Security Management Plan.
   3. In particular, the Supplier must, and ensure that all Subcontractors engaged in Development Activity:
      1. ensure that all Supplier Personnel engaged in Development Activity are:
         1. trained and experienced in secure by design code development;
         2. provided with regular training in secure software development and deployment;
      2. ensure that all Code:
         1. is subject to a clear, well organised, logical and documented architecture;
         2. follows OWASP Secure Coding Practice
         3. follows recognised secure coding standard, where one is available;
         4. employs consistent naming conventions;
         5. is coded in a consistent manner and style;
         6. is clearly and adequately documented to set out the function of each section of code;
         7. is subject to appropriate levels of review through automated and nonautomated methods both as part of:
            1. any original coding; and
            2. at any time the Code is changed;
      3. ensure that all Development Environments:
         1. protect access credentials and secret keys;
         2. is logically separate from all other environments, including production systems, operated by the Supplier or Subcontractor;
         3. requires multifactor authentication to access;
         4. have onward technical controls to protect the Developed System or the Supplier Information Management System in the event a Development Environment is compromised; and
         5. use network architecture controls to constrain access from the Development Environment to the Developed System or the Supplier Information Management System.
3. **Secure Architecture**
   1. The Supplier shall design and build the Developed System in a manner consistent with:
      1. the NCSC's guidance on "Security Design Principles for Digital Services";
      2. where the Developed System will Handle bulk data, the NCSC's guidance on "Bulk Data Principles"; and
      3. the NCSC's guidance on "Cloud Security Principles".
   2. Where any of the documents referred to in Paragraph 2.1 provides for various options, the Supplier must document the option it has chosen to implement and its reasons for doing so.
   3. Notwithstanding anything in the specification for the Developed System or this Contract, the Supplier must ensure that the Developed System encrypts Government Data:
      1. when the Government Data is stored at any time when no operation is being performed on it; and
      2. when the Government Data is transmitted.
   4. The Supplier must ensure that the Developed System is developed and configured so as to provide for the matters set out in Paragraphs 13.1 to 13.4 of the Security Requirements.
4. **Code Repository and Deployment Pipeline**
5. The Supplier must, and must ensure that all Subcontractors engaged in Development Activity:
   1. when using a cloud ‑based code repository for the deployment pipeline, use only a cloud ‑based code repository that has been assessed against the NCSC Cloud Security Principles;
   2. ensure user access to code repositories is authenticated using credentials, with passwords or private keys;
   3. ensure secret credentials are separated from source code; and
   4. run automatic security testing as part of any deployment of the Developed System.
6. **Development and Testing Data**
7. The Supplier must, and must ensure that all Subcontractors engaged in Development Activity, use only anonymised, dummy or synthetic data when using data within the Development Environment for the purposes of development and testing.
8. **Code Reviews**
   1. The Supplier must:
      1. regularly; or
      2. as required by the Authority
9. review the Code in accordance with the requirements of this Paragraph 5 ("**Code Review**").
   1. Before conducting any Code Review, the Supplier must agree with the Authority:
      1. the modules or elements of the Code subject to the Code Review;
      2. the development state at which the Code Review will take place;
      3. any specific security vulnerabilities the Code Review will assess; and
      4. the frequency of any Code Reviews,

(the "**Code Review Plan**").

* 1. For the avoidance of doubt the Code Review Plan may specify different modules or elements of the Code are reviewed at a different development state, for different security vulnerabilities and at different frequencies.
  2. The Supplier:
     1. must undertake Code Reviews in accordance with the Code Review Plan; and
     2. may undertake Code Reviews by automated means if this is consistent with the approach specified in the Code review Plan.
  3. No later than 10 Working Days after each Code Review, the Supplier must provide the Authority will a full, unedited and unredacted copy of the Code Review Report.
  4. Where the Code Review identifies any security vulnerabilities, the Supplier must:
     1. remedy these at its own cost and expense;
     2. ensure, so far as reasonably practicable, that the identified security vulnerabilities are not present in any other modules or code elements; and
     3. modify its approach to undertaking the Development Activities to ensure, so far as is practicable, the identified security vulnerabilities will not re‑occur; and
     4. provide the Authority with such information as it requests about the steps the Supplier takes under this Paragraph 5.6.

1. **Third-party Software**
2. The Supplier must not, and must ensure that Subcontractors do not, use any software to Handle Government Data where the licence terms of that software purport to grant the licensor rights to Handle the Government Data greater than those rights strictly necessary for the use of the software.
3. **Third-party Software Modules**
   1. Where the Supplier or a Subcontractor incorporates a Third party Software Module into the Code, the Supplier must:
      1. verify the source and integrity of the Third party Software Module by cryptographic signing or such other measure that provides the same level of assurance;
      2. perform adequate due diligence to determine whether there are any recognised security vulnerabilities with that Third party Software Module;
      3. continue to monitor any such Third-party Software Module so as to ensure it promptly becomes aware of any newly ‑discovered security vulnerabilities; and
      4. take appropriate steps to minimise the effect of any such security vulnerability on the Developed System.
   2. For the purposes of Paragraph 7.1(b), the Supplier must perform due diligence that is proportionate to the significance of the Third-party Software Module within the Code.
   3. The Supplier must produce and maintain a register of all Third-party Software Modules that form part of the Code ("**Modules Register**").
   4. The Modules Register must include, in respect of each Third-party Software Module:
      1. full details of the developer of the module;
      2. the due diligence the Supplier undertook on the Third-party Software Module before deciding to use it;
      3. any recognised security vulnerabilities in the Third-party Software Module; and
      4. how the Supplier will minimise the effect of any such security vulnerability on the Developed System.
   5. The Supplier must:
      1. review and update the Modules Register:
         1. within [10] Working Days of becoming aware of a security vulnerability in any Third-party Software Module; and
         2. at least once every 6 months; and
      2. provide the Authority with a copy of the Modules Register:
         1. whenever it updates the Modules Register; and
         2. otherwise when the Authority requests.
4. Security Working Group
5. **Role of the Security Working Group**
   1. The Security Working Group shall be responsible for the [insert remit of Security Working Group].
   2. The Security Working Group:
      1. monitors and provides recommendations to the Supplier on the [Authority-led Assurance] of the Supplier Information Management System;
      2. provides a forum for the sharing of information concerning security risks and threats and determining the appropriate mitigations;
      3. [insert remainder of terms of reference for Security Working Group].
6. **Meetings of the Security Working Group**
7. Paragraphs 3.4 to 3.7 of Schedule 17 (*Governance*) shall apply to the Security Working Group as if it were a Board established under that Schedule.
8. **Reports to the Security Working Group**
   1. The Supplier must provide the following reports no late than [5] Working Days before each meeting of the Security Woking Group:
      1. [insert list of required reports].
9. **Administration**
10. [The Supplier is responsible for the secretarial functions of the SWG.]
11. Subcontractor Security Requirements and Security Requirements for Development
    1. The table below sets out the Security Requirements and Development Requirements that do **not** apply to particular categories of Subcontractors.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | * 1. SIMS Subcontractors | * 1. Higher-risk Subcontractors | * 1. Medium-risk Subcontractors | * 1. Subcontractors |
| * 1. Security Requirements that do not apply |  |  |  |  |
| * 1. Development Requirements that do not apply |  |  |  |  |

1. Secure by Design Principles Evaluation Table
2. **Completion of Principles Evaluation Table**
   1. As part of the Security Management Plan, the Supplier must complete the table in this Appendix 5 (*Secure by Design Principles Evaluation Table*), unless that requirement is waived by the Authority.
   2. In completing this table, the Supplier must set out how it and any Subcontractors will meet the Secure by Design Principles.

| * 1. **Secure by Design Principle** | * 1. **Requirements** | * 1. **How the Supplier will meet the requirement** |
| --- | --- | --- |
| * 1. **Principle 1**   2. Create responsibility for cyber security risk   3. Assign a designated risk owner to be accountable for managing cyber security risks for the service within the contract. This must be a senior stakeholder with the experience, knowledge and authority to lead on security activities. | * 1. The Supplier designates a senior individual within their organisation who has overall accountability for ensuring the Secure by Design are met as part of the overall security requirements stated within the contract. |  |
| * 1. The Supplier designates a senior individual within the supplier delivery team - who will be reporting to the SRO, service owner or equivalent - with overall responsibility for the management of cyber security risks of digital services and technical infrastructure during their delivery. |  |
| * 1. The Supplier provides adequate and appropriately qualified resources to support the Authority with following the government [Secure by Design approach](https://www.security.gov.uk/guidance/secure-by-design/) as part of service delivery.   2. These resources must be reviewed at the beginning of each of the delivery phases during the delivery lifecycle of the service as agreed with the Authority. |  |
| * 1. **Principle 2**   2. Source secure technology products   3. Where third-party products are used, perform security due diligence by continually assessing platforms, software and code for security vulnerabilities. Mitigate risks and share findings with suppliers to help them improve product security. | * 1. The Supplier carries out proportionate (risk-driven) security reviews of third-party products before they are considered as a component of the digital service. The type and details of the review should be based on the significance associated with the product and are subject to agreement with the Authority. |  |
| * 1. The Supplier takes reasonable steps to reduce potential cyber security risks associated with using a third-party product as part of the service to a level that meets the Authority's security risk appetite for the service. Where the risk cannot be mitigated to such level, the Authority should be informed and asked to accept the risk associated with using the product. |  |
| * 1. The Supplier takes reasonable steps to assess third-party products used as a component of the digital service against legal and regulatory obligations and industry security standards specified by the Authority. Where the product doesn't meet the required obligations, the Supplier must discuss with the Authority the residual risks associated with using the product. |  |
| * 1. **Principle 3**   2. Adopt a risk-driven approach   3. Establish the project's risk appetite and maintain an assessment of cyber security risks to build protections appropriate to the evolving threat landscape. | * 1. As provided by the Authority, the Supplier should share the risk appetite across the supplier's delivery team from the outset. |  |
| * 1. The Supplier supports the Authority with identifying the cyber threats and attack paths as part of ongoing threat modelling during digital service delivery. |  |
| * 1. The Supplier supports the Authority with assessing cyber security risks and providing risk analysis details to help risk owners make informed risk decisions.   2. During the assessment, risks to the digital service are identified, analysed, prioritised, and appropriate mitigation is proposed taking into account the risk appetite during the lifecycle of the service. |  |
| * 1. The Supplier produces an output from the risk management process containing a clear set of security requirements that will reduce the risks in line with the agreed risk appetite and cyber security risk management approach. |  |
| * 1. The Supplier factors in the legal and regulatory requirements provided by the Authority in the risk management process and service design and build. |  |
| * 1. **Principle 4**   2. Design usable security controls   3. Perform regular user research and implement findings into service design to make sure security processes are fit for purpose and easy to understand. | * 1. The Supplier ensures that security requirements that are defined and documented as part of user research activities (for example user stories and user journeys) are fed into the design of the digital service. |  |
| * 1. The Supplier ensures that business objectives informing security requirements listed in the business case for the digital service are taken into consideration when designing security controls. |  |
| * 1. **Principle 5**   2. Build in detect and respond security   3. Design for the inevitability of security vulnerabilities and incidents. Integrate appropriate security logging, monitoring, alerting and response capabilities. These must be continually tested and iterated. | * 1. The Supplier responsible for building the digital service ensures that proportionate security logging, monitoring and alerting mechanisms able to discover cyber security events and vulnerabilities documented in the threat and risk assessment are designed into the service. |  |
| * 1. The Supplier responsible for building the digital service integrates incident response and recovery capabilities that are in line with the requirements and timescales documented in the service resilience or similar documentation. |  |
| * 1. The Supplier responsible for building the digital service regularly tests digital services and infrastructure to identify and fix weaknesses within systems. |  |
| * 1. **Principle 6**   2. Design flexible architectures   3. Implement digital services and update legacy components to allow for easier integration of new security controls in response to changes in business requirements, cyber threats and vulnerabilities. | * 1. As agreed with the Authority, the Supplier responsible for building the digital service uses flexible architectures and components that allow integration of new security measures in response to changes in business requirements, cyber threats and vulnerabilities. |  |
| * 1. The Supplier responsible for building the digital service tests security controls and verifying they are fit for purpose before deployment. |  |
| * 1. **Principle 7**   2. Minimise the attack surface   3. Use only the capabilities, software, data and hardware components necessary for a service to mitigate cyber security risks while achieving its intended use. | * 1. The Supplier responsible for building the digital service implements risk-driven security controls which meet the risk appetite and appropriate baseline as agreed with the Authority. |  |
| * 1. The Supplier responsible for building the digital service follows secure coding practices and, with consultation with the Authority's delivery team, identifies and mitigates vulnerabilities proactively reducing the number of vulnerabilities that potential attackers can exploit. |  |
| * 1. The Supplier retires service components (including data) securely when they are no longer needed, or at the end of their lifecycle. |  |
| * 1. **Principle 8**   2. Defend in depth   3. Create layered controls across a service so it's harder for attackers to fully compromise the system if a single control fails or is overcome. | * 1. The Supplier responsible for building the digital service adopts a defence in depth approach when designing the security architecture for the digital service. |  |
| * 1. The Supplier responsible for building the digital service implements security measures to incorporate segmentation. |  |

## Part B: Supplier-led Assurance

1. Authority Options
2. Where the Authority has selected an option in the table below, the Supplier must comply with the requirements relating to that option set out in the relevant Paragraph:

|  |  |  |
| --- | --- | --- |
| * 1. **Authority Security Policies** (see Paragraph 5) | | |
| * 1. The Authority requires the Supplier to comply with the following policies relating to security management: * [**List Authority security policies with which the Supplier and Subcontractors must comply]** | | * 1. ☐ |
| * 1. **Secure by Design Principles** (see Paragraph 14.6) | | |
| * 1. The Authority waives the requirement for the Security Management Plan to include an assessment of the Supplier Information Management System against the table in Appendix 6 (*Secure by Design Principles Evaluation Table*). | | * 1. ☐ |
| * 1. **Locations** (see Paragraph 1 of the Security Requirements) | | |
| * 1. The Supplier and Subcontractors may store, access or Handle Government Data in: | * 1. the United Kingdom only | * 1. ☐ |
| * 1. any territory as permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State) | * 1. ☐ |
| * 1. anywhere in the world not prohibited by the Authority | * 1. ☐ |
| * 1. **Support Locations** (see Paragraph 1 of the Security Requirements) | | |
| * 1. The Supplier and Subcontractors may operate Support Locations in: | * 1. the United Kingdom only | * 1. ☐ |
| * 1. any territory as permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State) | * 1. ☐ |
| * 1. anywhere in the world not prohibited by the Authority | * 1. ☐ |
| * 1. **Development Activity** (see Appendix 2 (*Security Requirements for Development*)) | | |
| * 1. The Authority requires the Supplier to undertake Development Activity under this Contract and, as a consequence, Appendix 2 (*Security Requirements for Development*) applies | | * 1. ☐ |
| * 1. **Locations for Development Activity** (applies only if the option relating to Development Activities is selected; see Paragraph 1 of the Security Requirements) | |  |
| * 1. The Supplier and Subcontractors may undertake Development Activity in: | * 1. the United Kingdom only | * 1. ☐ |
|  | * 1. any territory as permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State) | * 1. ☐ |
|  | * 1. anywhere in the world not prohibited by the Authority | * 1. ☐ |

1. Definitions

*[Guidance: Please note the following defined terms used within this Schedule can be found within Schedule 1 (Definitions): Assets, Authority Equipment, Authority Premises, Authority System, Code, Developed System, EEA, Government Data, Handle, Key Subcontractor, Malicious Software, Security Requirements, Security Requirements for Development, Sites.]*

|  |  |
| --- | --- |
| * 1. **"Anti‑virus Software"** | * 1. software that:      1. protects the Supplier Information Management System from the possible introduction of Malicious Software;      2. scans for and identifies possible Malicious Software in the Supplier Information Management System;      3. if Malicious Software is detected in the Supplier Information Management System, so far as possible:         1. prevents the harmful effects of the Malicious Software; and         2. removes the Malicious Software from the Supplier Information Management System; |
| * 1. **"Backup and Recovery Plan"** | * 1. the section of the Security Management Plan setting out the Suppliers' and Subcontractors' plans for the back and recovery of any Government Data they Handle; |
| * 1. **"Breach Action Plan"** | * 1. a plan prepared under Paragraph 16.3 of the Security Requirements addressing any Breach of Security; |
| * 1. **"Breach of Security"** | * 1. the occurrence of:      1. any unauthorised access to or use of the Services, the Authority Premises, the Sites, the Supplier Information Management System and/or any information or data used by the Authority, the Supplier or any Subcontractor in connection with this Contract, including the Government Data and the Code;      2. the loss (physical or otherwise), corruption and/or unauthorised disclosure of any information or data, including copies of such information or data, used by the Authority, the Supplier or any Subcontractor in connection with this Contract, including the Government Data and the Code; and/or      3. any part of the Supplier Information Management System ceasing to be compliant with the Certification Requirements;      4. the installation of Malicious Software in the:         1. Supplier Information Management System;         2. Development Environment; or         3. Developed System;      5. any loss of operational efficiency or failure to operate to specification as the result of the installation or operation of Malicious Software in the:         1. Supplier Information Management System;         2. Development Environment; or         3. Developed System; and      6. includes any attempt to undertake the activities listed in sub-Paragraph (a) of this definition where the Supplier has reasonable grounds to suspect that attempt:         1. was part of a wider effort to access information and communications technology operated by or on behalf of Central Government Bodies; or         2. was undertaken, or directed by, a state other than the United Kingdom; |
| * 1. **"Certification Requirements"** | * 1. the requirements set out in Paragraph 13; |
| * 1. **"CHECK Scheme"** | * 1. the NCSC's scheme under which approved companies can conduct authorised penetration tests of public sector and critical national infrastructure systems and networks; |
| * 1. **"CHECK Service Provider"** | * 1. a company which, under the CHECK Scheme:      1. has been certified by the National Cyber Security Centre;      2. holds "Green Light" status; and      3. is authorised to provide the IT Health Check services required by Paragraph 12 of the Security Requirements; |
| * 1. **"CHECK Team Leader"** | * 1. an individual with a CHECK Scheme team leader qualification issued by the NCSC; |
| * 1. **"CHECK Team Member"** | * 1. an individual with a CHECK Scheme team member qualification issued by the NCSC; |
| * 1. **"Code Review"** | * 1. a periodic review of the Code by manual or automated means to:      1. identify and fix any bugs; and      2. ensure the Code complies with         1. the requirements of this Schedule 5 (*Security Management*); and         2. the Secure Development Guidance; |
| * 1. **"Code Review Plan"** | * 1. the document agreed with the Authority under Paragraph 5.2 of the Security Requirements for Development setting out the requirements for, and frequency of, Code Reviews; |
| * 1. **"Code Review Report"** | * 1. a report setting out the findings of a Code Review; |
| * 1. **"Cyber Essentials"** | * 1. the Cyber Essentials certificate issued under the Cyber Essentials Scheme; |
| * 1. **"Cyber Essentials Plus"** | * 1. the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme; |
| * 1. **"Cyber Essentials Scheme"** | * 1. the Cyber Essentials scheme operated by the National Cyber Security Centre; |
| * 1. **"Data Migration Plan"** | * 1. the plan for the migration of the Government Data to the Authority and/or the Replacement Supplier (as required by the Authority) required by Paragraph 17 of the Security Requirements; |
| * 1. **"Development Activity"** | * 1. any activity relating to the development, deployment maintenance and upgrading of the Developed System, including:      1. coding;      2. testing;      3. code storage; and      4. deployment; |
| * 1. **"Development Environment"** | * 1. any information and communications technology system and the Sites forming part of the Supplier Information Management System that the Supplier or its Subcontractors will use to provide the Development Activity; |
| * 1. **"End-user Device"** | * 1. any personal computers, laptops, tablets, terminals, smartphones or other portable electronic device provided by the Supplier or a Subcontractor and used in the provision of the Services; |
| * 1. **"Email Service"** | * 1. a service that will send, or can be used to send, emails from the Authority's email address or otherwise on behalf of the Authority; |
| * 1. **"Expected Behaviours"** | * 1. the expected behaviours set out and updated from time to time in the Government Security Classification Policy, currently found at paragraphs 12 to 16 and in the table below paragraph 16 of <https://www.gov.uk/government/publications/government-security-classifications/guidance-11-working-at-official-html>; |
| * 1. **"Government Data Register"** | * 1. the register of all Government Data the Supplier, or any Subcontractor, receives from or creates for the Authority, produced and maintained in accordance with Paragraph 18 of the Security Requirements; |
| * 1. **"Government Security Classification Policy"** | * 1. the policy, as updated from time to time, establishing an administrative system to protect information assets appropriately against prevalent threats, including classification tiers, protective security controls and baseline behaviours, the current version of which is found at [https://www.gov.uk/ government/publications/government-security-classifications](https://www.gov.uk/government/publications/government-security-classifications/guidance-11-working-at-official-html); |
| * 1. **"Higher-risk Subcontractor"** | * 1. a Subcontractor that Handles Government Data, where that data includes either:      1. the Personal Data of 1000 or more individuals in aggregate during the period between the first Operational Service Commencement Date and the date on which this Contract terminates in accordance with Clause 4.1.2; or      2. any part of that Personal Data includes any of the following:         1. financial information (including any tax and/or welfare information) relating to any person;         2. any information relating to actual or alleged criminal offences (including criminal records);         3. any information relating to children and/or vulnerable persons;         4. any information relating to social care;         5. any information relating to a person's current or past employment; or         6. Special Category Personal Data; or      3. the Authority in its discretion, designates a Subcontractor as a Higher-risk Subcontractor:         1. in any procurement document related to this Contract; or         2. during the Term; |
| * 1. **"HMG Baseline Personnel Security Standard"** | * 1. the employment controls applied to any individual member of the Supplier Personnel that performs any activity relating to the provision or management of the Services, as set out in "HMG Baseline Personnel Standard", Version 7.0, June 2024 (<https://www.gov.uk/government/publications/government-baseline-personnel-security-standard>), as that document is updated from time to time; |
| * 1. **"Independent Security Adviser"** | the independent and appropriately qualified and experienced security architect or expert appointed under Paragraph 19; |
| * 1. **"ISO Certification"** | * 1. either of the following certifications when issued by a UKAS-recognised Certification Body:      1. ISO/IEC27001:2013, where the certification was obtained before November 2022, but only until November 2025; and      2. ISO/IEC27001:2022 in all other cases; |
| * 1. **"IT Health Check"** | * 1. testing of the Supplier Information Management System by a CHECK Service Provider. |
| * 1. **"Key Sub‑contractor Default"** | * 1. has the meaning set out in Paragraph 10.5; |
| * 1. **"Medium-risk Subcontractor"** | * 1. a Subcontractor that Handles Government Data, [where that data      1. includes the Personal Data of between 100 and 999 individuals (inclusive) in the period between the first Operational Service Commencement Date and the date on which this Contract terminates in accordance with Clause 4.1.2; and      2. does not include Special Category Personal Data]; |
| * 1. **"Modules Register"** | * 1. the register of Third-party Software Modules required by Paragraph 7.3 of the Security Requirements for Development; |
| * 1. **"NCSC"** | * 1. the National Cyber Security Centre or any replacement or successor body carrying out the same function; |
| * 1. **"NCSC Cloud Security Principles"** | * 1. the NCSC's document "Implementing the Cloud Security Principles" as updated or replaced from time to time and found at <https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles>; |
| * 1. **"NCSC Device Guidance"** | * 1. the NCSC's document "Device Security Guidance", as updated or replaced from time to time and found at <https://www.ncsc.gov.uk/collection/device-security-guidance>; |
| * 1. **"NCSC Protecting Bulk Personal Data Guidance"** | * 1. the NCSC's document "Protecting Bulk Personal Data", as updated or replaced from time to time and found at <https://www.ncsc.gov.uk/collection/protecting-bulk-personal-data>; |
| * 1. **"NCSC Secure Design Principles"** | * 1. the NCSC's document "Secure Design Principles", as updated or replaced from time to time and found at <https://www.ncsc.gov.uk/collection/cyber-security-design-principles/cyber-security-design-principles>; |
| * 1. **"OWASP"** | * 1. the Open Web Application Security Project Foundation; |
| * 1. **"OWASP Secure Coding Practice"** | * 1. the Secure Coding Practices Quick Reference Guide published by OWASP, as updated or replaced from time to time and found at <https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/>; |
| * 1. **"OWASP Top Ten"** | * 1. the list of the most critical security risks to web applications published annually by OWASP and found at <https://owasp.org/www-project-top-ten/>; |
| * 1. **"Privileged User"** | * 1. a user with system administration access to the Supplier Information Management System, or substantially similar access privileges; |
| * 1. **"Prohibited Activity"** | * 1. the storage, access or Handling of Government Data prohibited by a Prohibition Notice; |
| * 1. **"Prohibition Notice"** | * 1. a notice issued under Paragraph 1.11 of the Security Requirements; |
| * 1. **"Protective Monitoring System"** | * 1. the system implemented by the Supplier and its Subcontractors under Paragraph 14.1 of the Security Requirements to monitor and analyse access to and use of the Supplier Information Management System, the Development Environment, the Government Data and the Code; |
| * 1. **"RAP Trigger"** | * 1. the occurrence of one of the events set out in Paragraph 18.1; |
| * 1. **"Register of Sites, Support Locations and Third-party Tools"** | * 1. the part of the Security Management Plan setting out, in respect of Sites, Support Locations and Third-party Tools:      1. the Sites, Support Locations and Third-party Tools that the Supplier will use to Handle Government Data or provide the Services;      2. the nature of the activity performed at the Site or Support Location or by the Third-party Tool in respect of the Government Data;      3. in respect of each entity providing a Site, Support Location or Third-party Tool, its:         1. full legal name;         2. trading name (if any)         3. country of registration;         4. registration number (if applicable); and         5. registered address; |
| * 1. **"Relevant Activities"** | * 1. those activities specified in Paragraph 1.1 of the Security Requirements; |
| * 1. **"Relevant Certifications"** | * + 1. in the case of the Supplier, any SIMS Subcontractor and any Key Sub-contractor:        1. either:           1. an ISO Certification in respect of the Supplier Information Management System; or           2. where the Supplier Information Management System is included within the scope of a wider ISO Certification, that ISO Certification; and        2. Cyber Essentials Plus;     2. In the case of any Higher-risk Subcontractor, either:        1. an ISO Certification in respect of that part of the Supplier Information Management System provided by the Higher-risk Subcontractor;        2. where the that part of the Supplier Information Management System provided by the Higher-risk Subcontractor is included within the scope of a wider ISO Certification, that ISO Certification; or        3. Cyber Essentials Plus; and     3. in the case of any Medium-risk Subcontractors, means Cyber Essentials.   (or equivalent certifications); |
| * 1. **"Relevant Convictions"** | * 1. any previous or pending prosecution, conviction or caution (excluding any spent conviction under the Rehabilitation of Offenders Act 1974) relating to offences involving dishonesty, terrorism, immigration, firearms, fraud, forgery, tax evasion, offences against people (including sexual offences), or any other offences relevant to Services as the Authority may specify; |
| * 1. **"Remediation Action Plan"** | * 1. the plan prepared by the Supplier in accordance with Paragraph 18; |
| * 1. **"Remote Location"** | * 1. a location other than a Supplier's or a Subcontractor's Site; |
| * 1. **"Remote Working"** | * 1. the provision or management of the Services by Supplier Personnel from a location other than a Supplier's or a Subcontractor's Site; |
| * 1. **"Remote Working Policy"** | * 1. the policy prepared and approved under Paragraph 3.8 of the Security Requirements and forming part of the Security Management Plan under which Supplier Personnel are permitted to undertake Remote Working. |
| * 1. **"Required Changes Register"** | * 1. the register recording each of the changes that the Supplier proposes to the Supplier Information Management System or the Security Management Plan together with:      1. the details of any approval of the change provided by the Authority, including any conditions or limitations on that approval; and      2. the date:         1. the date by which the change it to be implemented; and         2. the date on which the change was implemented; |
| * 1. **"Residual Risk Statement"** | * 1. a notice issued by the Authority that      1. sets out the information risks associated with using the Supplier Information Management System; and      2. confirms that the Authority:         1. is satisfied that the identified risks have been adequately and appropriately addressed; and         2. that the residual risks are understood and accepted by the Authority; |
| * 1. **"Risk Management Approval Statement"** | * 1. the statement issued by the Authority under Paragraph 15.716.2 following the Authority's review of the Security Management Plan; |
| * 1. **"Secure by Design Principles"** | * 1. the Secure by Design Principles issued by the Cabinet Office, as updated or replaced from time-to-time, currently found at <https://www.security.gov.uk/policy-and-guidance/secure-by-design/principles/>; |
| * 1. **"Secure Development Guidance"** | * 1. the Supplier's secure coding policy required under its ISO27001 Relevant Certification; |
| * 1. **"Secure Location"** | * 1. has the meaning given to that term in Paragraph 2.1(a) of Appendix 1 (*Security Requirements*); |
| * 1. **"Security Controls"** | * 1. the security controls set out and updated from time to time in the Government Security Classification Policy, currently found at Paragraph 12 of <https://www.gov.uk/government/publications/government-security-classifications/guidance-15-considerations-for-security-advisors-html>; |
| * 1. **"Security Management Plan"** | * 1. the document prepared in accordance with the requirements of Paragraph 14 and in the format, and containing the information, specified in Appendix 5 (*Security Management Plan Template*); |
| * 1. **"Security Test"** | * + 1. an IT Health Check; or     2. a Supplier Security Test; |
| * 1. **"Security Working Group"** | the Board established under Paragraph 8 or Schedule 17 (*Governance*), as applicable; |
| * 1. **"SIMS Subcontractor"** | * 1. a Subcontractor designated by the Authority that provides or operates the whole, or a substantial part, of the Supplier Information Management System; |
| * 1. **"SMP Subcontractor"** | * 1. a Subcontractor that provides cloud-based services on a "one to many" basis, where such Subcontractor will not contract other than on their own contractual terms; |
| * 1. **"Statement of Information Risk Appetite"** | * 1. the statement provided by the Authority under Paragraph 14.1 setting out:      1. the nature and level of risk that the Supplier accepts from the operation of the Supplier Information Management System; and      2. the specific legal and regulatory requirements with which the Supplier must comply when Handling Government Data; |
| * 1. **"Subcontractor"** | * 1. for the purposes of this Schedule 5 (*Security Management*) only, any individual or entity that:      1. forms part of the supply chain of the Supplier; and      2. has access to, hosts, or performs any operation on or in respect of the Supplier Information Management System, the Development Environment, the Code and the Government Data,   2. and this definition shall apply to this Schedule 5 in place of the definition of Sub-contractor in Schedule 1 (*Definitions*); |
| * 1. **"Subcontractors' Systems"** | the information and communications technology system used by a Subcontractor in implementing and performing the Services, including:   * + 1. the Software;     2. the Supplier Equipment;     3. configuration and management utilities;     4. calibration and testing tools;     5. and related cabling; but   does not include the Authority System; |
| * 1. **"Supplier Information Management System"** | * + 1. the Supplier System;     2. the Sites;     3. any part of the Authority System the Supplier or any Subcontractor will use to Process Government Data, or provide the Services; and     4. the associated information management system, including all relevant:        1. organisational structure diagrams,        2. controls,        3. policies,        4. practices,        5. procedures,        6. processes; and        7. resources,   1. as determined by the Supplier after consultation with the Authority under Paragraph 11; |
| * 1. **"Supplier Personnel"** | * 1. for the purposes of this Schedule 5 (*Security Management*) only, any individual engaged, directly or indirectly, or employed by the Supplier or any Subcontractor (as that term is defined for the purposes of this Schedule 5 (*Security Management*)), in the management or performance of the Supplier's obligations under this Contract, and this definition shall apply to this Schedule 5 (*Security Management*) in place of the definition of Supplier Personnel in Schedule 1 (*Definitions*); |
| * 1. **"Support Location"** | * 1. a place or facility where or from which individuals may access or Handle the Code or the Government Data; |
| * 1. **"Support Register"** | * 1. the register of all hardware and software used to provide the Services produced and maintained in accordance with Paragraph 5 of the Security Requirements; |
| * 1. **"Third-party Software Module"** | * 1. any module, library or framework that:      1. is not produced by the Supplier or a Subcontractor as part of the Development Activity; and      2. either:         1. forms, or will form, part of the Code; or         2. is, or will be, accessed by the Developed System during its operation; |
| * 1. **"Third-party Tool"** | * 1. any Software used by the Supplier or a Subcontractor by which the Code or the Government Data is accessed, analysed or modified or some form of operation is performed on it; |
| * 1. **"UKAS"** | * 1. the United Kingdom Accreditation Service; |
| * 1. **"UKAS-recognised Certification Body"** | * + 1. an organisation accredited by UKAS to provide certification of ISO/IEC27001:2013 and/or ISO/IEC27001:2022; or     2. an organisation accredited to provide certification of ISO/IEC27001:2013 and/or ISO/IEC27001:2022 by a body with the equivalent functions as UKAS in a state with which the UK has a mutual recognition agreement recognising the technical equivalence of accredited conformity assessment; and |
| * 1. **"Wider Information Management System"** | * + 1. any:        1. information assets,        2. IT systems,        3. IT services; or Sites   that the Supplier or any Subcontractor will use to Handle, or support the Handling of, Government Data and provide, manage or support the provision of, the Services; and   * + 1. the associated information management system, including all relevant:        1. organisational structure diagrams,        2. controls,        3. policies,        4. practices,        5. procedures,        6. processes; and        7. resources. |

1. Introduction
2. This Schedule 5 (*Security Management*) sets out:
   1. the Authority's decision on where the Supplier may:
      1. store, access or Handle Government Data;
      2. undertake the Development Activity;
      3. host the Development Environment; and
      4. locate Support Locations,

(in Paragraph 1);

* 1. the principles of security that apply to this Contract (in Paragraph 4);
  2. the requirement to obtain a Risk Management Approval Statement (in Paragraphs 6 and 16);
  3. the annual confirmation of compliance to be provided by the Supplier (in Paragraph 7);
  4. the governance arrangements for security matters, where these are not otherwise specified in Schedule 17 (*Governance*) (in Paragraph 8);
  5. access to personnel (in Paragraph 9);
  6. obligations in relation to Subcontractors (in Paragraph 10);
  7. the responsibility of the Supplier to determine the Supplier Information Management System (in Paragraph 11);
  8. the Certification Requirements (in Paragraph 13);
  9. the development, monitoring and updating of the Security Management Plan by the Supplier (in Paragraphs 14, 15 and 16);
  10. the granting by the Authority of approval for the Supplier to commence:
      1. the provision of Operational Services; and/or
      2. Handling Government Data (in Paragraph 16);
  11. the management of changes to the Supplier Information Management System (in Paragraph 17); and
  12. the Authority's additional remedies for breach of this Schedule 5 (*Security Management*), including:
      1. the requirement for Remediation Action Plans (in Paragraph 18);
      2. the appointment of Independent Security Advisers (in Paragraph 19); and
      3. the withholding of Charges by the Authority (in Paragraph 20).

1. Principles of security
   1. The Supplier acknowledges that the Authority places great emphasis on the confidentiality, integrity and availability of the Government Data and, consequently, on the security of:
      1. the Authority System;
      2. the Supplier System;
      3. the Sites;
      4. the Services; and
      5. the Supplier Information Management System.
   2. The Parties shall share information and act in a co‑operative manner at all times to further the principles of security in Paragraph 4.1.
   3. Notwithstanding any approvals or agreements provided by the Authority under this Schedule 5 (*Security Management*), the Supplier remains responsible for:
      1. the security, confidentiality, integrity and availability of the Government Data when that Government Data is under the control of the Supplier or any of its Subcontractors; and
      2. the security of the Supplier Information Management System.
2. Security requirements
   1. The Supplier must, and must ensure that Subcontractors design, build and manage the Supplier Information Management System in accordance with the Security Management Plan.
   2. The Supplier must, unless otherwise agreed in writing with the Authority:
      1. comply with the Security Requirements in Appendix 1 (*Security Requirements*);
      2. where the relevant option in Paragraph 1 is selected, comply with the Security Requirements for Development in Appendix 2 (*Security Requirements for Development*);
      3. where the relevant option in Paragraph 1 is selected, comply with the Authority Security Policies; and
      4. ensure that Subcontractors comply with:
         1. all Security Requirements in Appendix 1 (*Security Requirements*);
         2. where the relevant option in Paragraph 1 is selected, all Security Requirements for Development in Appendix 2 (*Security Requirements for Development*); and
         3. where the relevant option in Paragraph 1 is selected, all Authority Security Policies,
         4. that apply to the activities that the Subcontractor performs under its Sub‑contract, unless:
         5. Paragraph 5.4 applies; or
         6. the table in Appendix 4 (*Subcontractor Security Requirements and Security Requirements for Development*) limits the Security Requirements or Security Requirements for Development that apply to a Subcontractor.
   3. Where the Authority selects the option in Paragraph 1 requiring the Supplier to comply with the Authority Security Policies, if there is an inconsistency between the Authority Security Requirements and the requirement of this Schedule 5 (*Security Management*), then the requirements of this Schedule 5 (*Security Management*) will prevail to the extent of that inconsistency.
   4. Where a Subcontractor is a SMP Subcontractor, the Supplier shall:
      1. use reasonable endeavours to ensure that the SMP Subcontractor complies with all obligations that this Schedule 5 (*Security Management*) imposes on Subcontractors, including the Security Requirements;
      2. document the differences between those obligations and the obligations that the SMP Subcontractor is prepared to accept in sufficient detail to allow the Authority to form an informed view of the risks concerned; and
      3. take such steps as the Authority may require to mitigate those risks.
3. Authority to proceed
4. Notwithstanding anything in this Contract, the Supplier may not:
   1. commence the provision of any Operational Services; or
   2. Handle any Government Data using the Supplier Information Management System,

unless

* 1. the Supplier has, and ensured that Subcontractors have, obtained the Relevant Certifications under Paragraph 13;
  2. the Supplier has completed an IT Health Check in accordance with Paragraph 12 of the Security Requirements; and
  3. the Authority has issued a Risk Management Approval Statement under Paragraph 16.2.

1. Supplier confirmation
   1. The Supplier must, no later than the last day of each Contract Year, provide to the Authority a letter from its [chief executive officer] (or equivalent officer) confirming that, having made due and careful enquiry:
      1. the Supplier has in the previous year carried out all tests and has in place all procedures required in relation to security matters required by this Contract;
      2. subject to Paragraph 7.2:
         1. it has fully complied with all requirements of this Schedule 5 (*Security Management*); and
         2. all Subcontractors have complied with the requirements of this Schedule 5 (*Security Management*) with which the Supplier is required to ensure they comply; and
      3. the Supplier considers that its security and risk mitigation procedures remain effective.
   2. Where the Authority has, in respect of the period covered by the confirmation provided under Paragraph 7.1 agreed in writing that the Supplier need not, or need only partially, comply within any requirement of this Schedule 5 (*Security Management*):
      1. the confirmation must include details of the Authority's agreement; and
      2. confirm that the Supplier has fully complied with that modified requirement.
   3. The Supplier must:
      1. keep and maintain a register setting out all agreements referred to in Paragraph 7.2; and
      2. provide a copy of that register to the Authority on request.
2. Governance, information sharing and co-operation

Governance

* 1. Paragraphs 8.1 to 8.8 apply where a Security Working Group, or Board (as that term is defined in Schedule 17 (*Governance*)), with a similar remit, is not provided for otherwise in this Contract.
  2. The Authority must establish a Security Working Group on which both the Authority and the Supplier are represented.
  3. The notice or other document establishing the Security Working Group must set out:
     1. the Authority members;
     2. the Supplier members;
     3. the chairperson of the Security Working Group;
     4. the date of the first meeting;
     5. the frequency of meetings; and
     6. the location of meetings.
  4. The Security Working Group has oversight of all matters relating to the security of the Government Data and the Supplier Information Management System.
  5. The Security Working Group meets:
     1. at least once every 3 months; and
     2. additionally when required by the Authority.
  6. The Supplier must ensure that the Supplier Personnel attending each meeting of the Security Working Group:
     1. have sufficient knowledge and experience to contribute to the discussion of the matters on the agenda for the meeting;
     2. are authorised to make decisions that are binding on the Supplier in respect of those matters, including any decisions that require expenditure or investment by the Supplier; and
     3. where relevant to the matters on the agenda for the meeting, include representatives of relevant Subcontractors.
  7. Any decisions, recommendations or advice of the Security Working Group:
     1. are binding on the Supplier, unless:
        1. the Authority agrees otherwise; or
        2. the decision, recommendation or advice of the Security Working Group imposes on the Supplier more onerous requirements than those provided for in this Schedule 5 (*Security Management*); and
     2. do not limit or modify the Supplier's responsibilities under this Schedule 5 (*Security Management*).
  8. Appendix 3 (*Security Working Group*) applies to the Security Working Group.

1. Personnel
   1. The Supplier must ensure that at all times it maintains within the Supplier Personnel sufficient numbers of qualified, skilled security professionals to ensure the Supplier complies with the requirements of this Schedule 5 (*Security Management*).
   2. The Supplier must appoint:
      1. a senior individual within its organisation with accountability for managing security risks and the Supplier's implementation of the requirements of this Schedule 5 (*Security Management*); and
      2. a senior individual within the team responsible for the delivery of the Services with responsibility for managing the security risks to the Supplier Information Management System.
   3. The individuals appointed under Paragraph 9.2:
      1. must have sufficient experience, knowledge and authority to undertake their roles effectively; and
      2. are to be designated as Key Personnel and treated for the purposes of this Contract as Key Personnel, whether or not they are otherwise designated as such;
   4. The Supplier must review, and if necessary replace, the individuals appointed under Paragraph 9.2 if required to do so by the Authority.
   5. To facilitate:
      1. the Authority's oversight of the Supplier Information Management System; and
      2. the Supplier's design, implementation, operation, management and continual improvement of the Security Management Plan and the security of the Services and Supplier Information Management System and otherwise,
   6. at reasonable times and on reasonable notice:
      1. the Supplier shall provide access to the Supplier Personnel responsible for information assurance; and
      2. the Authority shall provide access to its personnel responsible for information assurance.
2. Subcontractors
   1. Paragraphs 10.2 to 10.4 are subject to Paragraph 5.4.

SIMS Subcontractor

* 1. A SIMS Subcontractor shall be treated for all purposes as a Key Sub‑contractor.
  2. In addition to the obligations imposed by this Contract on Key Sub‑contractors, the Supplier must ensure that the Key Subcontract with each SIMS Subcontractor contains obligations no less onerous on the Key Sub-contractor than those imposed on the Supplier under this Schedule 5 (*Security Management*).

Subcontractors

* 1. The Supplier must, before entering into a binding Sub‑contract with any Subcontractor:
     1. undertake sufficient due diligence of the proposed Subcontractor to provide reasonable assurance that the proposed Subcontractor can perform the obligations that this Schedule 5 (*Security Management*) requires the Supplier ensure that the proposed Subcontractor performs;
     2. keeps adequate records of the due diligence it has undertaken in respect of the proposed Subcontractors; and
     3. provides those records to the Authority on request.

Key Sub‑contractor Default

* 1. Where the Supplier becomes aware of an actual or suspected failure by a Key Sub‑contractor to comply with any obligation in this Schedule 5 (*Security Management*) with which the Supplier is, by virtue of Paragraph 5.2.1, required to ensure the Key Sub‑contractor complies ("**Key Sub‑contractor Default**"), the Supplier must:
     1. as soon as reasonably practicable and in any event within 2 Working days of becoming aware of the Key Sub‑contractor Default notify the Authority setting out the actual or anticipated effect of the Key Sub‑contractor Default; and
     2. unless the Authority waives the requirement, comply with the Remediation Action Plan process in Paragraph 18.

1. Supplier Information Management System
   1. The Supplier must determine:
      1. the scope and component parts of the Supplier Information Management System; and
      2. the boundary between the Supplier Information Management System and the Wider Information Management System.
   2. Before making its determination under Paragraph 11.1, the Supplier must consult with the Authority and in doing so must provide the Authority with such documentation and information that the Authority may require regarding the Wider Information Management System.
   3. The Supplier shall reproduce its decision under Paragraph 11.1 as a diagram documenting the components and systems forming part of, and the boundary between, the Supplier Information Management System and the Wider Information Management System.
   4. The diagram prepared under Paragraph 11.3 forms part of the Security Management Plan.
   5. Any proposed change to:
      1. the component parts of the Supplier Information Management System; or
      2. the boundary between the Supplier Information Management System and the Wider Information Management System,

is:

* + 1. an Operational Change to which the Change Control Procedure applies; and
    2. requires approval by the Authority under Paragraph 17; and
    3. the Authority may require the appointment of an Independent Security Adviser to advise on the proposed change.

1. Government Data Handled using Supplier Information Management System
   1. The Supplier acknowledges that the Supplier Information Management System:
      1. is intended only for the Handling of Government Data that is classified as OFFICIAL; and
      2. is not intended for the Handling of Government Data that is classified as SECRET or TOP SECRET,

in each case using the Government Security Classification Policy.

* 1. The Supplier must:
     1. not alter the classification of any Government Data; and
     2. if it becomes aware that any Government Data classified as SECRET or TOP SECRET is being Handled using the Supplier Information Management System:
        1. immediately inform the Authority; and
        2. follow any instructions from the Authority concerning that Government Data.
  2. The Supplier must, and must ensure that Subcontractors and Supplier Personnel, when Handling Government Data, comply with:
     1. the Expected Behaviours; and
     2. the Security Controls.
  3. Where there is a conflict between the Expected Behaviours or the Security Controls and this Schedule 5 (*Security Management*) the provisions of this Schedule 5 (*Security Management*) shall apply to the extent of any conflict.

1. Certification Requirements
   1. The Supplier shall ensure that, unless otherwise agreed by the Authority, both:
      1. it; and
      2. any SIMS Subcontractor, any Key Sub-contractor, any Higher-risk Subcontractor and any Medium-risk Subcontractor,
   2. are certified as compliant with the Relevant Certifications, that is to say:
      1. in the case of the Supplier, any SIMS Subcontractor and any Key Sub‑contractor:
         1. either:
            1. an ISO Certification in respect of the Supplier Information Management System; or
            2. where the Supplier Information Management System is included within the scope of a wider ISO Certification, that ISO Certification; and
         2. Cyber Essentials Plus;
         3. (or equivalent); and
      2. in the case of any Higher-risk Subcontractor, either:
         1. an ISO Certification in respect of that part of the Supplier Information Management System provided by the Higher-risk Subcontractor; or
         2. where that part of the Supplier Information Management System provided by the Higher-risk Subcontractor is included within the scope of a wider ISO Certification, that ISO Certification; or
         3. Cyber Essentials Plus; and
      3. in the case of any Medium-risk Subcontractor, Cyber Essentials (or equivalent).
   3. Unless otherwise agreed by the Authority, before it begins to provide the Services, the Supplier must provide the Authority with a copy of:
      1. the Relevant Certifications for it and any Subcontractor; and
      2. the relevant scope and statement of applicability required under the ISO/IEC 27001 Relevant Certifications.
   4. The Supplier must ensure that at the time it begins to provide the Services, the Relevant Certifications for it and any Subcontractor are:
      1. currently in effect;
      2. together cover at least the full scope of the Supplier Information Management System; and
      3. are not subject to any condition that may impact the provision of the Services or the Development Activity ("**Certification Requirements**").
   5. The Supplier must notify the Authority promptly, and in any event within 3 Working Days, after becoming aware that, in respect of it or any Subcontractor:
      1. a Relevant Certification in respect of the Supplier Information Management System has been revoked or cancelled by the body that awarded it;
      2. a Relevant Certification in respect of the Supplier Information Management System has expired and has not been renewed by the Supplier;
      3. the Relevant Certifications together no longer apply to the full scope of the Supplier Information Management System; or
      4. the body that awarded a Relevant Certification has made it subject to conditions, the compliance with which may impact the provision of the Services (each a "**Certification Default**").
   6. Where the Supplier has notified the Authority of a Certification Default under Paragraph 13.5:
      1. the Supplier must, within ten Working Days of the date in which the Supplier provided notice under Paragraph 13.5 (or such other period as the Parties may agree) provide a draft plan ("**Certification Rectification Plan**") to the Authority setting out:
         1. full details of the Certification Default, including a root cause analysis;
         2. the actual and anticipated effects of the Certification Default;
         3. the steps the Supplier and any Subcontractor to which the Certification Default relates will take to remedy the Certification Default; and
      2. the Authority must notify the Supplier as soon as reasonably practicable whether it accepts or rejects the Certification Rectification Plan; and
      3. if the Authority rejects the Certification Rectification Plan, the Supplier must within 5 Working Days of the date of the rejection submit a revised Certification Rectification Plan and Paragraph 13.6.2 will apply to the re‑submitted plan;
      4. the rejection by the Authority of a revised Certification Rectification Plan is a material Default of this Contract; and
      5. if the Authority accepts the Certification Rectification Plan, the Supplier must start work immediately on the plan.
2. Security Management Plan

Purpose of Security Management Plan

* 1. The Authority may, at any time, provide the Supplier with a Statement of Information Risk Appetite.
  2. The Supplier must document in the Security Management Plan how the Supplier and its Subcontractors will:
     1. comply with the requirements set out in this Schedule 5 (*Security Management*) and the Contract in order to ensure the security of the Government Data and the Supplier Information Management System; and
     2. ensure that the operation of the Supplier Information Management System and the provision of the Services does not give rise to any information security risks greater than those set out in that Statement of Information Risk Appetite (where one has been provided).
  3. The Supplier must ensure that:
     1. the Security Management Plan accurately represents the Supplier Information Management System;
     2. the Supplier Information Management System will meet the requirements of this Schedule 5 (*Security Management*) and the Statement of Information Risk Appetite (where one has been provided); and
     3. the residual risks of the Supplier Information Management System are no greater than those provided for in the Statement of Information Risk Appetite (where one has been provided).

Preparation of Security Management Plan

* 1. The Supplier must prepare and submit the Security Management Plan to the Authority:
     1. by the date specified in the Detailed Implementation Plan; or
     2. if no such date is specified, in sufficient time to allow for the Authority review and approve the Security Management Plan before the first Operational Service Commencement Date.
  2. If Paragraph 14.4.2 applies, and any delay resulting from the Authority's review and approval of the Security Management Plan (including any additional activity required by the Supplier to ensure the Security Management Plan complies with Paragraph 14.3) causes or contributes to Supplier Non-Performance under Clause 29.1 that delay is not an Authority Cause and the Supplier shall not be entitled to any relief or compensation under Clause 29.

Contents of Security Management Plan

* 1. The Security Management Plan must include:
     1. a formal information risk assessment of, and a risk treatment plan for, the Supplier Information Management System;
     2. a completed statement of applicability under the relevant ISO Certification for the Supplier Information Management System;
     3. the process for managing any security risks from Subcontractors and third parties with access to the Services, the Supplier Information Management System or the Government Data;
     4. unless the Authority has waived this requirement by selecting the relevant option in Paragraph 1, an assessment of the Supplier Information Management System against the table in Appendix 6 (*Secure by Design Principles Evaluation Table*);
     5. unless such requirement is waived by the Authority, the controls the Supplier will implement in respect of the Services and all processes associated with the delivery of the Services, including:
        1. the Supplier System;
        2. the Sites; and
        3. the Authority System (to the extent that it is under the control of the Supplier); and
        4. any IT, Information and data (including the Confidential Information of the Authority and the Government Data) to the extent used by the Authority or the Supplier:
           1. in connection with this Contract or
           2. in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Services;
     6. the Required Changes Register;
     7. evidence that the Supplier and each Subcontractor (so far as those requirements apply) is compliant with:
        1. the Certification Requirements;
        2. the Security Requirements; and
        3. where the relevant option in Paragraph 1 is selected, the Security Requirements for Development;
     8. the diagram documenting the Supplier Information Management System, the Wider Information Management System and the boundary between them (created under Paragraph 11);
     9. an assessment of the Supplier Information Management System against the requirements of this Schedule 5 (*Security Management*), including the Security Requirements and, where the relevant option in Paragraph 1 is selected, the Security Requirements for Development (where applicable);
     10. the process the Supplier will implement immediately after it becomes aware of a Breach of Security to restore normal operations as quickly as possible, minimising any adverse impact on the Government Data, the Authority, the Services and/or users of the Services; and
     11. the following information, so far as is applicable, in respect of each Subcontractor:
         1. the Subcontractor's:
            1. legal name;
            2. trading name (if any); and
            3. registration details (where the Subcontractor is not an individual);
         2. the Relevant Certifications held by the Subcontractor;
         3. the Sites used by the Subcontractor;
         4. the Services provided, or contributed to, by the Subcontractor;
         5. the access the Subcontractor has to the Supplier Information Management System;
         6. the Government Data Handled by the Subcontractor;
         7. the Handling that the Subcontractor will undertake in respect of the Government Data; and
         8. the measures the Subcontractor has in place to comply with the requirements of this Schedule 5 (*Security Management*); and
         9. the due diligence the Supplier has taken to assess that compliance;
     12. the Register of Sites, Support Locations and Third-party Tools;
     13. the Modules Register;
     14. the Support Register;
     15. the Backup and Recovery Plan;
     16. the Remote Working Policy (where the Supplier or a Subcontractor proposes to allow Supplier Personnel to work from a Remote Location); and
     17. details of the protective monitoring that the Supplier will undertake in accordance with Paragraph 14 of the Security Requirements, including:
         1. the additional audit and monitoring the Supplier will undertake of the Supplier Information Management System; and
         2. the retention periods for audit records and event logs.

1. Monitoring and updating Security Management Plan

Updating Security Management Plan

* 1. The Supplier shall regularly review and update the Security Management Plan, and provide such to the Authority, at least once each year and as required by this Paragraph.

Monitoring

* 1. The Supplier, where it plans to undertake, or after becoming aware of, any of the following:
     1. a significant change to the components or architecture of the Supplier Information Management System;
     2. a significant change in the boundary between the Supplier Information Management System and the Wider Information Management System
     3. a significant change in the operation of the Supplier Information Management System;
     4. the replacement of an existing, or the appointment of a new:
        1. SIMS Subcontractor; or
        2. Subcontractor that Handles Government Data;
     5. a significant change in the quantity of Personal Data held within the Service; and/or
     6. where the Supplier or a Subcontractor has previously Handled Government Data that is Personal Data, other than Special Category Personal Data, it proposes to start to Handle Government Data that is Special Category Personal Data under this Contract;

must:

* + 1. within 2 Working Days notify the Authority; and
    2. within 10 Working Days, or such other timescale as may be agreed with the Authority:
       1. update the Required Changes Register and any other affected parts of the Security Management Plan; and
       2. provide the Authority with a copy those documents for review and approval.
  1. Paragraph 15.2 applies in addition to, and not in substitution of, the Parties obligations to comply with the Change Control Procedure for any Contract Change or Operational Change.
  2. Any proposed change under Paragraph 15.2.1, 15.2.2 or 15.2.6 constitutes a Contract Change to which the Change Control Procedure applies.

1. Review and approval of updated Security Management Plan
   1. Where the Supplier has prepared or updated the Security Management Plan the Authority may review the plan and to do so may request such further information as the Authority considers necessary or desirable.
   2. At the conclusion of that review, it may issue to the Supplier:
      1. where satisfied that the:
         1. identified risks to the Supplier Information Management System are adequately and appropriately addressed; and
         2. that the residual risks are:
            1. either:

where the Authority has provided a Statement of Information Risk Appetite, reduced to the level anticipated by that statement; or

where the Authority has not provided a Statement of Information Risk Appetite, reduced to an acceptable level;

* + - * 1. understood and accepted by the Authority; and
        2. recorded in the Residual Risk Statement;

a Risk Management Approval Statement; or

* + 1. where the Authority reasonably considers that:
       1. the identified risks to the Supplier Information Management System have not been adequately or appropriately addressed; or
       2. the residual risks to the Supplier Information Management System have not been reduced:
          1. where the Authority has Provided a Statement of Information Risk Appetite, to the level anticipated by that statement; or
          2. where the Authority has not Provided a Statement of Information Risk Appetite, to an acceptable level,

a Risk Management Rejection Notice, with the reasons for its decision.

1. Changes to the Supplier Information Management System
   1. Notwithstanding anything in this Contract, the Supplier must obtain the approval of the Authority before making any of the following changes to the Supplier Information Management System:
      1. a significant change in the systems or components making up the Supplier Information Management System;
      2. a significant change in the operation or management of the Supplier Information Management System; or
      3. the appointment of a new, or the replacement of an existing:
         1. SIMS Subcontractor; or
         2. Subcontractor that Handles Government Data.
   2. In seeking the Authority's approval to a proposed changes to the Supplier Information Management System, the Supplier must:
      1. update the Required Changes Register;
      2. prepare a proposal for the Authority setting out:
         1. details of the proposed changes to the Supplier Information Management System;
         2. an assessment of the security implications of the proposed change;
         3. a risk assessment of the proposed change; and
         4. any proposed changes to the Security Management Plan; and
      3. provide that paper to the Authority no later than 30 Working Days before the date on which it will consider the proposed changes.
   3. The Authority:
      1. may request such further information as the Authority considers necessary or desirable;
      2. must provide its decision within 20 Working Days of the later of:
         1. the date on which it receives the proposal; or
         2. the date on which it receives any requested further information; and
      3. must not:
         1. unreasonably refuse any proposal by the Supplier; and
         2. must not make any approval subject to unreasonable conditions.
   4. If the Authority does not provide a decision within the period specified in Paragraph 17.3.1, the proposal shall be deemed to have been accepted.

Implementation of changes

* 1. Where the Supplier implements a necessary change to the Supplier Information Management System to address a security related risk or vulnerability, the Supplier shall effect such change at its own cost and expense.
  2. If the Supplier does not implement a necessary change to the Supplier Information Management System to address a security related risk or vulnerability by the date set out in the Required Changes Register:
     1. that failure is a material Default; and
     2. the Supplier shall:
        1. immediately cease using the Supplier Information Management System to Handle Government Data either:
           1. until the Default is remedied, or
           2. unless directed otherwise by the Authority in writing and then only in accordance with the Authority's written directions; and
        2. where such material Default is capable of remedy, remedy such material Default within the timescales set by the Authority (considering the security risks the material Default presents to the Services and/or the Supplier Information Management System).

1. Remediation Action Plan

Preparation of Remediation Action Plan

* 1. This Paragraph 18 applies when:
     1. Key Sub‑contractor Default occurs;
     2. the Authority issues a Risk Management Rejection Notice; or
     3. the Supplier receives a Security Test report identifies vulnerabilities in, or makes findings in respect of, the Supplier Information Management System,

(each a **RAP Trigger**).

* 1. The Supplier must within [20] Working Days of the occurrence of a RAP Trigger prepare and submit for approval to the Authority a draft plan (**Remediation Action Plan**).
  2. The draft Remediation Action Plan must, in respect of each issue raised by the RAP Trigger, set out:
     1. full details of that issue;
     2. the actual or anticipated effect of that issue;
     3. how the issue will be remedied;
     4. the date by which the issue will be remedied; and
     5. the tests that the Supplier proposes to perform to confirm that the issue has been remedied.

Consideration of Remediation Action Plan

* 1. The Supplier must
     1. provide the Authority with a copy of any Remediation Action Plan it prepares;
     2. have regarded to any comments the Authority provides in respect of the Remediation Action Plan; and
     3. fully implement the Remediation Action Plan according to its terms.

Implementing an approved Remediation Action Plan

* 1. In implementing the Remediation Action Plan, the Supplier must conduct such further tests on the Supplier Information Management System as are required by the Remediation Action Plan to confirm that the Remediation Action Plan has fully and correctly implemented.
  2. If any such testing identifies a new risk, new threat, vulnerability or exploitation technique with the potential to affect the security of the Supplier Information Management System, the Supplier shall within [2] Working Days of becoming aware of such risk, threat, vulnerability or exploitation technique:
     1. provide the Authority with a full, unedited and unredacted copy of the test report;
     2. implement interim mitigation measures to vulnerabilities in the Information System known to be exploitable where a security patch is not immediately available; and
     3. as far as practicable, remove or disable any extraneous interfaces, services or capabilities not needed for the provision of the Services within the timescales set out in the test report or such other timescales as may be agreed with the Authority.

1. Independent Security Adviser
   1. The Authority may require the appointment of an Independent Security Adviser where:
      1. there is a proposed change to the Supplier Information Management System (see Paragraph 11.5);
      2. the Authority issues two or more Risk Management Rejection Notices (see Paragraph 16.2); or
      3. either:
         1. a Security Test report identifies more than ten vulnerabilities classified as either critical or high; or
         2. the Authority rejected a revised draft Remediation Action Plan (see Paragraph 12.21 of Appendix 1 (*Security Requirements*)).
   2. Where the Authority requires the appointment of an Independent Security Adviser the Independent Security Adviser shall be:
      1. a person selected by the Supplier and approved by the Authority; or
      2. where:
         1. the Authority does not approve the persons selected by the Supplier; or
         2. the Supplier does not select any person within ten Working Days of the date of the notice requiring the Independent Security Adviser's appointment,

a person selected by the Authority.

* 1. The terms of the Independent Security Adviser's appointment shall require that person to:
     1. undertake a detailed review, including a full root cause analysis where the Independent Security Adviser considers it appropriate to do so, of the circumstances that led to that person's appointment; and
     2. provide advice and recommendations on:
        1. steps the Supplier can reasonably take to improvement the security of the Supplier Information Management System; and
        2. where relevant, how the Supplier may mitigate the effects of, and remedy, those and to avoid the occurrence of similar circumstances to those leading to the appointment of the Independent Security Adviser in the future.
  2. The Supplier must permit, and must ensure that relevant Subcontractors permit, the Independent Security Adviser to:
     1. observe the conduct of and work alongside the Supplier Personnel to the extent that the Independent Security Adviser considers reasonable and proportionate having regard to reason for their appointment;
     2. gather any information the Independent Security Adviser considers relevant in the furtherance of their appointment;
     3. write reports and provide information to the Authority in connection with the steps being taken by the Supplier to remedy the matters leading to the Independent Security Adviser's appointment;
     4. make recommendations to the Authority and/or the Supplier as to how the matters leading to their appointment might be mitigated or avoided in the future; and/or
     5. take any other steps that the Authority and/or the Independent Security Adviser reasonably considers necessary or expedient in order to mitigate or rectify matters leading to the Independent Security Adviser's appointment.
  3. The Supplier must, and ensure that relevant Subcontractors:
     1. where relevant, work alongside, provide information to, co‑operate in good faith with and adopt any reasonable methodology in providing the Services recommended by the Independent Security Adviser in order to mitigate or rectify any of the vulnerabilities that led to the appointment of the Independent Security Adviser;
     2. ensure that the Independent Security Adviser has all the access it may require in order to carry out its objective, including access to the Assets;
     3. submit to such monitoring as the Authority and/or the Independent Security Adviser considers reasonable and proportionate in respect of the matters giving rise to their appointment;
     4. implement any recommendations (including additional security measures and/or controls) made by the Independent Security Adviser that have been approved by the Authority within the timescales given by the Independent Security Adviser; and
     5. not terminate the appointment of the Independent Security Adviser without the prior consent of the Authority (unless such consent has been unreasonably withheld).
  4. The Supplier shall be responsible for:
     1. the costs of appointing, and the fees charged by, the Independent Security Adviser; and
     2. its own costs in connection with any action required by the Authority and/or the Independent Security Adviser.
  5. If the Supplier or any relevant Subcontractor:
     1. fails to perform any of the steps required by the Authority in the notice appointing the Independent Security Adviser; and/or
     2. is in Default of any of its obligations under this Paragraph 19,

this is a material Default that is not capable of remedy.

1. Withholding of Charges
   1. The Authority may withhold some or all of the Charges in accordance with the provisions of this Paragraph 20 where:
      1. the Supplier in in material Default of any of its obligations under this Schedule 5 (*Security Management*); or
      2. any of the following matters occurs (where the those matters arise from a Default by the Supplier of its obligations under this this Schedule 5 (*Security Management*)):
         1. a Notifiable Default;
         2. an Intervention Cause; or
         3. a Step-In Trigger Event.
   2. The Authority may withhold an amount of the Charges that it considers sufficient, in its sole discretion, to incentivise the Supplier to perform the obligations it has Defaulted upon.
   3. Before withholding any Charges under Paragraph 20.1 the Authority must
      1. provide written notice to the Supplier setting out:
         1. the Default in respect of which the Authority has decided to withhold some or all of the Charges;
         2. the amount of the Charges that the Authority will withhold;
         3. the steps the Supplier must take to remedy the Default;
         4. the date by which the Supplier must remedy the Default;
         5. the invoice in respect of which the Authority will withhold the Charges; and
      2. consider any representations that the Supplier may make concerning the Authority's decision.
   4. Where the Supplier does not remedy the Default by the date specified in the notice given under Paragraph 20.3.1, the Authority may retain the withheld amount.
   5. The Supplier acknowledges:
      1. the legitimate interest that the Authority has in ensuring the security of the Supplier Information Management System and the Government Data and, as a consequence, the performance by the Supplier of its obligations under this Schedule 5 (*Security Management*); and
      2. that any Charges that are retained by the Authority are not out of all proportion to the Authority's legitimate interest, even where:
         1. the Authority has not suffered any Losses as a result of the Supplier's Default; or
         2. the value of the Losses suffered by the Authority as a result of the Supplier's Default is lower than the amount of the Charges retained.
   6. The Supplier may raise a Dispute under the Dispute Resolution Procedure with any decision by the Authority to:
      1. withhold any Charges under Paragraph 20.1; or
      2. retain any Charges under Paragraph 20.4.
   7. Any Dispute raised by the Supplier does not prevent the Authority withholding Charges in respect of:
      1. the decision subject to the Dispute; or
      2. any other matter to which this Paragraph 20 applies.
   8. Where any Dispute raised by the Supplier is resolved wholly or partially in its favour, the Authority must return such sums as are specified in any agreement or other document setting out the resolution of the Dispute.
   9. The Authority's right to withhold or retain any amount under this Paragraph 20 are in addition to any other rights that the Authority may have under this Contract or in Law, including any right to claim damages for Losses it suffers arising from the Default.
2. Access to Authority System
   1. Where the Supplier, a Subcontractor or any of the Supplier Personnel is granted access to the Authority System or to the Authority Equipment, it must comply with and ensure that all such Subcontractors and Supplier Personnel comply with, all rules, policies and guidance provided to it and as updated from time to time concerning the Authority System or the Authority Equipment.

appendix 1 Security Requirements

1. **Location**

Location for Relevant Activities

* 1. Unless otherwise agreed with the Authority, the Supplier must, and ensure that its Subcontractors, at all times:
     1. provide the Services;
     2. undertake any activity supporting or managing:
        1. the Services;
        2. the Supplier Information Management System; or
        3. the Wider Information Management System;
     3. store, access or Handle Government Data;
     4. undertake the Development Activity; and
     5. host the Wider Information Management System, including any Sites
  2. (together, the "**Relevant Activities**")
  3. only in or from the geographic areas permitted by the Authority in Paragraph 1.
  4. Where the Authority has not selected an option concerning location in Paragraph 1, the Supplier may only undertake the Relevant Activities in or from:
     1. the United Kingdom; or
     2. a territory permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State).
  5. The Supplier must, and must ensure that its Subcontractors undertake the Relevant Activities in a facility operated by an entity where:
     1. the entity has entered into a binding agreement with the Supplier or Subcontractor (as applicable);
     2. that binding agreement includes obligations on the entity in relation to security management equivalent to those imposed on Subcontractors in this Schedule 5 (*Security Management*);
     3. the Supplier or Subcontractor has taken reasonable steps to assure itself that the entity complies with the binding agreement;
     4. the Supplier has provided the Authority with such information as the Authority requires concerning:
        1. the entity;
        2. the arrangements with the entity; and
        3. the entity's compliance with the binding agreement; and
     5. the Authority has not given the Supplier a Prohibition Notice under Paragraph 1.11.
  6. Where the Supplier cannot comply with one or more of the requirements of Paragraph 1.3:
     1. it must provide the Authority with such information as the Authority requests concerning:
        1. the security controls in places at the relevant location or locations; and
        2. where certain security controls are not, or only partially, implemented the reasons for this;
     2. the Authority may grant approval to use that location or those locations, and that approval may include conditions; and
     3. if the Authority does not grant permission to use that location or those locations, the Supplier must, within such period as the Authority may specify:
        1. cease to store, access or Handle Government Data at that location or those locations;
        2. sanitise, in accordance with instructions from the Authority, such equipment within the information and communications technology system used to store, access or Handle Government Data at that location, or those locations, as the Authority may specify.

Support Locations

* 1. The Supplier must ensure that all Support Locations are located only in the geographic areas permitted by the Authority.
  2. Where the Authority has not selected an option concerning location in Paragraph 1, the Supplier may only locate Support Locations in:
     1. the United Kingdom; or
     2. a territory permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State).
  3. The Supplier must, and must ensure that its Subcontractors operate the Support Locations in a facility operated by an entity where:
     1. the entity has entered into a binding agreement with the Supplier or Subcontractor (as applicable);
     2. the binding agreement includes obligations on the entity in relation to security management equivalent to those relating to Subcontractors in this Schedule 5 (*Security Management*);
     3. the Supplier or Subcontractor has taken reasonable steps to assure itself that the entity complies with the binding agreement;
     4. the Supplier has provided the Authority with such information as the Authority requires concerning:
        1. the entity;
        2. the arrangements with the entity; and
        3. the entity's compliance with the binding agreement; and
     5. the Authority has not given the Supplier a Prohibition Notice under Paragraph 1.11.

Third-party Tools

* 1. Before using any Third-party Tool, the Supplier must, and must ensure that its Subcontractors:
     1. perform adequate due diligence to determine whether there are any recognised security vulnerabilities with that Third-party Tool;
     2. the Supplier has provided the Authority with such information as the Authority requires concerning:
        1. the arrangements with the provider of the Third-party Tool; and
        2. the due diligence undertaken by the Supplier or Subcontractor; and
     3. do not use a Third-party Tool in respect of which the Authority has given the Supplier a Prohibition Notice under Paragraph 1.11.
  2. The Supplier must use, and ensure that Subcontractors use, only those Third-party Tools included in the Register of Sites, Support Locations and Third-party Tools.
  3. The Supplier must not, and must not allow Subcontractors to, use:
     1. a Third-party Tool other than for the activity specified for that Third-party Tool in the Register of Sites, Support Locations and Third-party Tools; or
     2. a new Third-party Tool, or replace an existing Third-party Tool, without the permission of the Authority.

Prohibited Activities

* 1. The Authority may by notice in writing at any time give notice to the Supplier that it and its Subcontractors must not:
     1. undertake or permit to be undertaken some or all of the Relevant Activities or operate Support Locations ("**Prohibited Activity**").
        1. in any particular country or group of countries;
        2. in or using facilities operated by any particular entity or group of entities; or
        3. in or using any particular facility or group of facilities, whether operated by the Supplier, a Subcontractor or a third‑party entity; or
     2. use any specified Third-party Tool,

(a **Prohibition Notice**).

* 1. Where the Supplier or Subcontractor, on the date of the Prohibition Notice:
     1. undertakes any Prohibited Activities;
     2. operates any Support Locations; or
     3. employs any Third-party Tool,

affected by the notice, the Supplier must, and must procure that Subcontractors, cease to undertake that Prohibited Activity or employ that Third-party Tool within 40 Working Days of the date of the Prohibition Notice.

1. Physical Security
   1. The Supplier must ensure, and must ensure that Subcontractors ensure, that:
      1. all Sites, locations at which Relevant Activities are performed, or Support Locations ("**Secure Locations**") have the necessary physical protective security measures in place to prevent unauthorised access, damage and interference, whether malicious or otherwise, to Government Data;
      2. the operator of the Secure Location has prepared a physical security risk assessment and a site security plan for the Secure Location; and
      3. the physical security risk assessment and site security plan for each Secure Location:
         1. considers whether different areas of the Secure Location require different security measures based on the functions of each area;
         2. adopts a layered approach to physical security;
         3. has sections dealing with the following matters:
            1. the perimeter of the Secure Location;
            2. the building fabric;
            3. security guarding;
            4. visitor and people management;
            5. server and communications rooms;
            6. protection of sensitive data;
            7. closed circuit television;
            8. automated access and control systems;
            9. intruder detection; and
            10. security control rooms.
   2. The Supplier must provide the Authority with the physical security risk assessment and site security plan for any Secure Location within 20 Working Days of a request by the Authority.
2. **Vetting, Training and Staff Access**

Vetting before performing or managing Services

* 1. The Supplier must not engage Supplier Personnel, and must ensure that Subcontractors do not engage Supplier Personnel in:
     1. any activity relating to the provision or management of the Services; or
     2. any activity that allows or requires the Handling of Government Data,

unless:

* + 1. that individual has passed the security checks listed in Paragraph 3.2; or
    2. the Authority has given prior written permission for a named individual to perform a specific role.
  1. For the purposes of Paragraph 3.1, the security checks are:
     1. The checks required for the HMG Baseline Personnel Security Standard (BPSS) to verify:
        1. the individual's identity;
        2. where that individual will work in the United Kingdom, the individual's nationality and immigration status so as to demonstrate that they have a right to work in the United Kingdom;
        3. the individual's previous employment history; and
        4. that the individual has no Relevant Convictions;
     2. national security vetting clearance to the level specified by the Authority for such individuals or such roles as the Authority may specify; or
     3. such other checks for the Supplier Personnel of Subcontractors as the Authority may specify.

Exception for certain Subcontractors

* 1. Where the Supplier considers it cannot ensure that a Subcontractor will undertake the relevant security checks on any Supplier Personnel, it must:
     1. as soon as practicable, and in any event within [20] Working Days of becoming aware of the issue, notify the Authority;
     2. provide such information relating to the Subcontractor, its vetting processes and the roles the affected Supplier Personnel will perform as the Authority reasonably requires; and
     3. comply, at the Supplier's cost, with all directions the Authority may provide concerning the vetting of the affected Supplier Personnel and the management of the Subcontractor.

Annual training

* 1. The Supplier must ensure, and ensure that Subcontractors ensure, that all Supplier Personnel, complete and pass security training at least once every calendar year that covers:
     1. general training concerning security and data handling;
     2. Phishing, including the dangers from ransomware and other malware; and
     3. the Secure by Design Principles.

Staff access

* 1. The Supplier must ensure, and ensure that Subcontractors ensure, that individual Supplier Personnel can access only the Government Data necessary to allow individuals to perform their role and fulfil their responsibilities in the provision of the Services.
  2. The Supplier must ensure, and ensure that Subcontractors ensure, that where individual Supplier Personnel no longer require access to the Government Data or any part of the Government Data, their access to the Government Data or that part of the Government Data is revoked immediately when their requirement to access Government Data ceases.
  3. Where requested by the Authority, the Supplier must remove, and must ensure that Subcontractors remove, an individual Supplier Personnel's access to the Government Data, or part of that Government Data specified by the Authority, as soon as practicable and in any event within 24 hours of the request.

Remote Working

* 1. The Supplier must ensure, and ensure that Subcontractors ensure, that:
     1. unless in writing by the Authority, Privileged Users do not undertake Remote Working;
     2. where the Authority permits Remote Working by Privileged Users, the Supplier ensures, and ensures that Subcontractors ensure, that such Remote Working takes place only in accordance with any conditions imposed by the Authority.
  2. Where the Supplier or a Subcontractor wishes to permit Supplier Personnel to undertake Remote Working, it must:
     1. prepare and have approved by the Authority the Remote Working Policy in accordance with this Paragraph;
     2. undertake and, where applicable, ensure that any relevant Subcontractors undertake, all steps required by the Remote Working Policy;
     3. ensure that Supplier Personnel undertake Remote Working only in accordance with the Remote Working Policy; and
     4. may not permit any Supplier Personnel of the Supplier or any Subcontractor to undertake Remote Working until the Remote Working Policy is approved by the Authority.
  3. The Remote Working Policy must include or make provision for the following matters:
     1. restricting or prohibiting Supplier Personnel from printing documents in any Remote Location;
     2. restricting or prohibiting Supplier Personnel from downloading any Government Data to any End-user Device other than an End User Device that:
        1. is provided by the Supplier or Subcontractor (as appropriate); and
        2. complies with the requirements set out in Paragraph 4 (*End-user Devices*);
     3. ensuring that Supplier Personnel comply with the Expected Behaviours (so far as they are applicable);
     4. giving effect to the Security Controls (so far as they are applicable);
     5. for each different category of Supplier Personnel subject to the proposed Remote Working Policy:
        1. the types and volumes of Government Data that the Supplier Personnel can Handle in a Remote Location and the Handling that those Supplier Personnel will undertake;
        2. any identified security risks arising from the proposed Handling in a Remote Location;
        3. the mitigations, controls and security measures the Supplier or Subcontractor (as applicable) will implement to mitigate the identified risks;
        4. the residual risk levels following the implementation of those mitigations, controls and measures;
        5. when the Supplier or Subcontractor (as applicable) will implement the proposed mitigations, controls and measures; and
        6. the business rules with which the Supplier Personnel must comply; and
     6. how the Supplier or the Subcontractor (as applicable) will:
        1. communicate the Remote Working Policy and business rules to Supplier Personnel; and
        2. enforce the Remote Working Plan and business rules.
  4. The Supplier may submit a proposed Remote Working Policy to the Authority for consideration at any time.
  5. The Authority must, within 20 Working Days of the submission of a proposed Remote Working Plan, either:
     1. approve the proposed Remote Working Policy, in which case the Supplier must, and ensure that any applicable Subcontractor, implements the approved Remote Working Plan in accordance with its terms; or
     2. reject the proposed Remote Working Policy, in which case:
        1. the Authority may set out any changes to the proposed Remote Working Policy the Authority requires to make the plan capable of approval; and
        2. the Supplier may:
           1. revise the proposed Remote Working Plan; and
           2. re-submit the proposed Remote Working Plan to the Authority for approval under Paragraph 3.11.

1. **End-user Devices**
   1. The Supplier must manage, and must ensure that all Subcontractors manage, all End-user Devices on which Government Data or Code is stored or Handled in accordance the following requirements:
      1. the operating system and any applications that store, Handle or have access to Government Data or Code must be in current support by the vendor, or the relevant community in the case of open source operating systems or applications;
      2. users must authenticate before gaining access;
      3. all Government Data and Code must be encrypted using an encryption tool agreed to by the Authority;
      4. the End-user Device must lock and require any user to re‑authenticate after a period of time that is proportionate to the risk environment, during which the End-user Device is inactive;
      5. the End-user Device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Government Data and Code to ensure the security of that Government Data and Code;
      6. the Suppler or Subcontractor, as applicable, can, without physical access to the End-user Device, remove or make inaccessible all Government Data or Code stored on the device and prevent any user or group of users from accessing the device; and
      7. all End-user Devices are within the scope of any Relevant Certification.
   2. The Supplier must comply, and ensure that all Subcontractors comply, with the recommendations in NCSC Device Guidance as if those recommendations were incorporated as specific obligations under this Contract.
   3. Where there is any conflict between the requirements of this Schedule 5 (*Security Management*) and the requirements of the NCSC Device Guidance, the requirements of this Schedule 5 (*Security Management*) take precedence.
2. **Hardware and software support**
   1. Before using any software as part of the Supplier Information Management System, the Supplier must:
      1. perform adequate due diligence to determine whether there are any recognised security vulnerabilities with that software; and
      2. where there are any recognised security vulnerabilities, either:
         1. remedy vulnerabilities; or
         2. ensure that the design of the Supplier Information Management System mitigates those vulnerabilities.
   2. The Supplier must ensure that all software used to provide the Services remains at all times in full security support, including any extended or bespoke security support.
   3. The Supplier must produce and maintain a register of all software that forms the Supplier Information Management System ("**Support Register**").
   4. The Support Register must include in respect of each item of software:
      1. any vulnerabilities identified with the software and the steps the Supplier has taken to remedy or mitigate those vulnerabilities;
      2. the date, so far as it is known, that the item will cease to be in mainstream security support; and
      3. the Supplier's plans to upgrade the item before it ceases to be in mainstream security support.
   5. The Supplier must:
      1. review and update the Support Register:
         1. within 10 Working days of becoming aware of any new vulnerability in any item of software;
         2. within 10 Working Days of becoming aware of the date on which, or any change to the date on which, any item of software will cease to be in mainstream security report;
         3. within 10 Working Days of introducing new software, or removing existing software, from the Supplier Information Management System; and
         4. at least once every 12 months; and
      2. provide the Authority with a copy of the Support Register:
         1. whenever it updates the Support Register; and
         2. otherwise when the Authority requests.
   6. Where any element of the Supplier Information Management System consists of COTS Software, the Supplier shall ensure:
      1. those elements are always in mainstream or extended security support from the relevant vendor; and
      2. the COTS Software is not more than one version or major release behind the latest version of the software.
   7. The Supplier shall ensure that all hardware used to provide the Services, whether used by the Supplier or any Subcontractor is, at all times, remains in mainstream vendor support, that is, that in respect of the hardware, the vendor continues to provide:
      1. regular firmware updates to the hardware; and
      2. a physical repair or replacement service for the hardware.
   8. The Supplier must ensure that where any software or hardware component of the Supplier Information Management System is no longer required to provide the Services or has reached the end of its life it is removed or disconnected from the Supplier Information Management System.
3. **Encryption**
   1. Before Handling any Government Data, the Supplier must agree with the Authority the encryption methods that it and any Subcontractors that Handle Government Data will use to comply with this Paragraph 6.
   2. Where this Paragraph 6 requires Government Data to be encrypted, the Supplier must use, and ensure that Subcontractors use, the methods agreed by the Authority under Paragraph 6.1.
   3. Unless Paragraph 6.4 applies, the Supplier must ensure, and must ensure that all Subcontractors ensure, that Government Data is encrypted:
      1. when stored at any time when no operation is being performed on it, including when stored on any portable storage media; and
      2. when transmitted.
   4. Where the Supplier, or a Subcontractor, cannot encrypt Government Data as required by Paragraph 6.2, the Supplier must:
      1. immediately inform the Authority of the subset or subsets of Government Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;
      2. provide details of the protective measures the Supplier or Subcontractor (as applicable) proposes to take to provide equivalent protection to the Authority as encryption; and
      3. provide the Authority with such additional information relating to the information provided under sub-Paragraphs (a) and (b) as the Authority may require.
   5. The Authority, the Supplier and, where the Authority requires, any relevant Subcontractor shall meet to agree appropriate protective measures for the unencrypted Government Data.
   6. Where the Authority and Supplier reach agreement, the Supplier must update the Security Management Plan to include:
      1. the subset or subsets of Government Data not encrypted and the circumstances in which that will occur; and
      2. the protective measure that the Supplier and/or Subcontractor will put in place in respect of the unencrypted Government Data.
   7. Where the Authority and Supplier do not reach agreement within 40 Working Days of the date on which the Supplier first notified the Authority that it could not encrypt certain Government Data, either party may refer the matter to [be determined by an expert in accordance with the Dispute Resolution Procedure].
4. **Backup and recovery of Government Data**

Backups and recovery of Government Data

* 1. The Supplier must backup and recover the Government Data in accordance with the Backup and Recovery Plan to ensure the recovery point objective and recovery time objective in Paragraph 7.3(a).
  2. Any backup system operated by the Supplier or Subcontractor forms part of the Supplier System or that Subcontractor's System to which this Schedule 5 (*Security Management*) and the Security Requirements apply.

Backup and Recovery Plan

* 1. Unless otherwise required by the Authority, the Backup and Recovery Plan must provide for:
     1. in the case of a full or partial failure of the Supplier System or a Subcontractor's System:
        1. a recovery time objective of [**insert period**]; and
        2. a recovery point objective of [**insert period**]; and
     2. a retention period of [**insert period**].
  2. In doing so, the Backup and Recovery Plan must ensure that in respect of any backup system operated by the Supplier or a Subcontractor:
     1. the backup location for Government Data is sufficiently physically and logically separate from the rest of the Supplier System or a Subcontractor's System that it is not affected by any Disaster affecting the rest of the Supplier System or a Subcontractor's System;
     2. there is sufficient storage volume for the amount of Government Data to be backed up;
     3. all back-up media for Government Data is used in accordance with the manufacturer's usage recommendations;
     4. newer backups of Government Data do not overwrite existing backups made during the retention period specified in Paragraph 7.3(a)(ii);
     5. the backup system monitors backups of Government Data to:
        1. identifies any backup failure; and
        2. confirm the integrity of the Government Data backed up;
     6. any backup failure is remedied promptly;
     7. the backup system monitors the recovery of Government Data to:
        1. identify any recovery failure;
        2. confirm the integrity of Government Data recovered; and
     8. any recovery failure is promptly remedied.

1. **Email**
   1. The Supplier must ensure that where the Supplier Information Management System will provide an Email Service to the Authority, it:
      1. supports transport layer security ("**TLS**") version 1.2, or higher, for sending and receiving emails;
      2. supports TLS Reporting ("**TLS‑RPT**");
      3. is capable of implementing:
         1. domain ‑based message authentication, reporting and conformance ("**DMARC**");
         2. sender policy framework ("**SPF**"); and
         3. domain keys identified mail ("**DKIM**"); and
      4. is capable of complying in all respects with any guidance concerning email security as issued or updated from time to time by:
         1. the UK Government (current version at <https://www.gov.uk/guidance/set-up-government-email-services-securely>; or
         2. the NCSC (current version at <https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing>).
2. **DNS**

Unless otherwise agreed by the Authority, the Supplier must ensure that the Supplier Information Management System uses the UK public sector Protective DNS ("**PDNS**") service to resolve internet DNS queries.

1. **Malicious Software**
   1. The Supplier shall install and maintain Anti‑virus Software or procure that Anti‑virus Software is installed and maintained on the Supplier Information Management System.
   2. The Supplier must ensure that such Anti‑virus Software:
      1. prevents the installation of the most common forms of Malicious Software in the Supplier Information Management System and the Development Environment;
      2. is configured to perform automatic software and definition updates;
      3. provides for all updates to be the Anti‑virus Software to be deployed within [10] Working Days of the update's release by the vendor;
      4. performs regular scans of the Supplier Information Management System to check for and prevent the introduction of Malicious Software; and
      5. where Malicious Software has been introduced into the Supplier Information Management System, identifies, contains the spread of, and minimises the impact of Malicious Software.
   3. If Malicious Software is found, the Parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Government Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.
   4. Any Breach of Security caused by Malicious Software where the Breach of Security arose from a failure by the Supplier, or a Subcontractor, to comply with this Paragraph 10 is a material Default.
2. **Vulnerabilities**
   1. Unless the Authority otherwise agrees, the Supplier must ensure that it or any relevant Subcontractor applies security patches to any vulnerabilities in the Supplier Information Management System no later than:
      1. 7 days after the public release of patches for vulnerabilities classified as "critical";
      2. 30 days after the public release of patches for vulnerabilities classified as "important"; and
      3. 60 days after the public release of patches for vulnerabilities classified as "other".
   2. The Supplier must:
      1. scan the Supplier Information Management System and the Development Environment at least once every month to identify any unpatched vulnerabilities; and
      2. if the scan identifies any unpatched vulnerabilities ensure they are patched in accordance with Paragraph 11.1.
   3. For the purposes of this Paragraph 11, the Supplier must implement a method for classifying vulnerabilities to the Supplier Information Management System as "critical", "important" or "other" that is aligned to recognised vulnerability assessment systems, such as:
      1. the National Vulnerability Database's vulnerability security ratings; or
      2. Microsoft's security bulletin severity rating system.
3. **Security testing**

Responsibility for security testing

* 1. The Supplier is solely responsible for:
     1. the costs of conducting any security testing required by this Paragraph 12; and
     2. the costs of implementing any findings, or remedying any vulnerabilities, identified in that security testing.

Security tests by Supplier

* 1. The Supplier must:
     1. before submitting the draft Security Management Plan to the Authority for a decision under Paragraph **15** of this Schedule 5 *(Security Management)*;
     2. at least once during each Contract Year; and
     3. when required to do so by the Authority;
     4. undertake the following activities:
        1. conduct security testing of the Supplier Information Management System (**IT Health Check**) in accordance with Paragraphs 12.8 to 12.10; and
        2. implement any findings, and remedy any vulnerabilities identified by the IT Health Check in accordance with Paragraphs 12.11 to 12.21.
  2. In addition to its obligations under Paragraph 12.2, the Supplier must undertake any tests required by:
     1. any Remediation Action Plan;
     2. the ISO27001 Certification Requirements;
     3. the Security Management Plan; and
     4. the Authority, following a Breach of Security or a significant change, as assessed by the Authority, to the components or architecture of the Supplier Information Management System,

(each a Supplier Security Test).

* 1. The Supplier must:
     1. design and implement the Supplier Security Tests so as to minimise the impact on the delivery of the Services;
     2. agree the date, timing, content and conduct of such Supplier Security Tests in advance with the Authority.
  2. Where the Supplier fully complies with Paragraph 12.4, if a Supplier Security Test causes a Performance Failure in a particular Measurement Period, the Supplier shall be entitled to relief in respect of such Performance Failure for that Measurement Period.
  3. The Authority may send a representative to witness the conduct of the Supplier Security Tests.
  4. The Supplier shall provide the Authority with a full, unedited and unredacted copy of the results of such Security Tests (in a form approved by the Authority in advance) as soon as practicable, and in any case within 10 Working Days, after completion of each Supplier Security Test.

IT Health Checks

* 1. In arranging an IT Health Check, the Supplier must:
     1. use only a CHECK Service Provider to perform the IT Health Check;
     2. ensure that the CHECK Service Provider uses a qualified CHECK Team Leader and CHECK Team Members to perform the IT Health Check;
     3. design and plan for the IT Health Check so as to minimise the impact of the IT Health Check on the Supplier Information Management System and the delivery of the Services.
     4. promptly provide the Authority with such technical and other information relating to the Information Management System as the Authority requests;
     5. include within the scope of the IT Health Check such tests as the Authority requires; and
     6. agree with the Authority the scope, aim and timing of the IT Health Check.
  2. The Supplier must commission the IT Health Check in accordance with the scope, aim and timing agreed by the Authority.
  3. Following completion of an IT Health Check, the Supplier must provide the Authority with a full, unedited and unredacted copy of the report relating to the IT Health Check without delay and in any event within ten Working Days of its receipt by the Supplier.

Remedying vulnerabilities

* 1. In addition to complying with Paragraphs 12.13 to 12.21, the Supplier must remedy:
     1. any vulnerabilities classified as critical in a Security Test report within five Working Days of becoming aware of the vulnerability and its classification;
     2. any vulnerabilities classified as high in a Security Test report within one month of becoming aware of the vulnerability and its classification; and
     3. any vulnerabilities classified as medium in a Security Test report within 3 months of becoming aware of the vulnerability and its classification.
  2. The Supplier must notify the Authority immediately if it does not, or considers it will not be able to, remedy the vulnerabilities classified as critical, high or medium in a Security Test report within the time periods specified in Paragraph 12.11.

Responding to a Security Test report

* 1. Where the Security Test report identifies vulnerabilities in, or makes findings in respect of, the Supplier Information Management System, the Supplier must within [20] Working Days of receiving the Security Test report, prepare and submit for approval to the Authority a draft plan addressing the vulnerabilities and findings ("**Remediation Action Plan**").
  2. Where the Authority has commissioned a root cause analysis under Paragraph 12.21, the Supplier shall ensure that the draft Remediation Action Plan addresses that analysis.
  3. The draft Remediation Action Plan must, in respect of each vulnerability identified or finding made by the Security Test report:
     1. how the vulnerability or finding will be remedied;
     2. the date by which the vulnerability or finding will be remedied; and
     3. the tests that the Supplier proposes to perform to confirm that the vulnerability has been remedied or the finding addressed.
  4. The Supplier shall promptly provide the Authority with such technical and other information relating to the Supplier Information Management System, the IT Health Check report or the draft Remediation Action Plan as the Authority requests.
  5. The Authority may:
     1. reject the draft Remediation Action Plan where it considers that the draft Remediation Action Plan is inadequate, providing its reasons for doing so, in which case:
        1. the Supplier shall within 10 Working Days of the date on which the Authority rejected the draft Remediation Action Plan submit a revised draft Remediation Action Plan that takes into account the Authority's reasons; and
        2. Paragraphs 12.15 to 12.17 shall apply, with appropriate modifications, to the revised draft Remediation Action Plan;
     2. accept the draft Remediation Action Plan, in which case the Supplier must immediately start work on implementing the Remediation Action Plan in accordance with Paragraphs 12.19 and 12.20.
  6. Where the Authority unreasonably:
     1. delays its approval; or
     2. rejects,

the draft Remediation Action Plan, the Supplier will not be in breach of this Contract to the extent it demonstrates that any breach:

* + 1. arose directly from the Authority unreasonably withholding or delaying, as appropriate, its approval of the draft Remediation Action Plan; and
    2. would not have occurred had:
       1. the Authority given its approval, or given its approval in a timely manner, to the draft Remediation Action Plan; and
       2. the Supplier had implemented the draft Remediation Action Plan in accordance with its terms.

Implementing an approved Remediation Action Plan

* 1. In implementing the Remediation Action Plan, the Supplier must conduct such further tests on the Supplier Information Management System as are required by the Remediation Action Plan to confirm that the Remediation Action Plan has fully and correctly implemented.
  2. If any such testing identifies a new risk, new threat, vulnerability or exploitation technique with the potential to affect the security of the Supplier Information Management System, the Supplier shall within 2 Working Days of becoming aware of such risk, threat, vulnerability or exploitation technique:
     1. provide the Authority with a full, unedited and unredacted copy of the test report;
     2. implement interim mitigation measures to vulnerabilities in the Information System known to be exploitable where a security patch is not immediately available; and
     3. as far as practicable, remove or disable any extraneous interfaces, services or capabilities not needed for the provision of the Services within the timescales set out in the test report or such other timescales as may be agreed with the Authority.

Significant vulnerabilities

* 1. Where:
     1. a Security Test report identifies more than 10 vulnerabilities classified as either critical or high; or
     2. the Authority rejected a revised draft Remediation Action Plan,

the Authority may, at the Supplier's cost, either:

* + 1. appoint an independent and appropriately qualified and experienced security architect and adviser to perform a root cause analysis of the identified vulnerabilities; or
    2. give notice to the Supplier requiring the appointment as soon as reasonably practicable, and in any event within 10 Working Days, of an Independent Security Adviser.

1. **Access Control**
   1. The Supplier must, and must ensure that all Subcontractors:
      1. identify and authenticate all persons who access the Supplier Information Management System and Sites before they do so;
      2. require multi‑factor authentication for all user accounts that have access to Government Data or that are Privileged Users;
      3. allow access only to those parts of the Supplier Information Management System and Sites that those persons require; and
      4. maintain records detailing each person's access to the Supplier Information Management System and Sites, and make those records available to the Authority on request.
   2. The Supplier must ensure, and must ensure that all Subcontractors ensure, that the user accounts for Privileged Users of the Supplier Information Management System:
      1. are allocated to a single, individual user;
      2. are accessible only from dedicated End-user Devices;
      3. are configured so that those accounts can only be used for system administration tasks;
      4. require passwords with high complexity that are changed regularly;
      5. automatically log the user out of the Supplier Information Management System after a period of time that is proportionate to the risk environment during which the account is inactive; and
      6. are:
         1. restricted to a single role or small number of roles;
         2. time limited; and
         3. restrict the Privileged User's access to the internet.
   3. The Supplier must ensure, and must ensure that all Subcontractors ensure, that it logs all activity of the Privileged Users while those users access those accounts and keeps the activity logs for 20 Working Days before deletion.
   4. The Supplier must require, and must ensure that all Subcontractors require, that Privileged Users use unique and substantially different high ‑complexity passwords for their different accounts on the Supplier Information Management System.
   5. The Supplier must, and must ensure that all Subcontractors:
      1. configure any hardware that forms part of the Supplier Information Management System that is capable of requiring a password before it is accessed to require a password; and
      2. change the default password of that hardware to a password of high complexity that is substantially different from the password required to access similar hardware.
2. **Event logging and protective monitoring**

Protective Monitoring System

* 1. The Supplier must, and must ensure that Subcontractors, implement an effective system of monitoring and reports, analysing access to and use of the Supplier Information Management System, the Development Environment, the Government Data and the Code to:
     1. identify and prevent potential Breaches of Security;
     2. respond effectively and in a timely manner to Breaches of Security that do occur;
     3. identify and implement changes to the Supplier Information Management System to prevent future Breaches of Security; and
     4. help detect and prevent any potential criminal offence relating to fraud, bribery or corruption using the Supplier Information Management System,

("**Protective Monitoring System**").

* 1. The Protective Monitoring System must provide for:
     1. event logs and audit records of access to the Supplier Information Management system; and
     2. regular reports and alerts to identify:
        1. changing access trends;
        2. unusual usage patterns; or
        3. the access of greater than usual volumes of Government Data;
     3. the detection and prevention of any attack on the Supplier Information Management System or the Development Environment using common cyber‑attack techniques; and
     4. any other matters required by the Security Management Plan.

Event logs

* 1. The Supplier must ensure that, unless the Authority otherwise agrees, any event logs do not log:
     1. personal data, other than identifiers relating to users; or
     2. sensitive data, such as credentials or security keys.

Provision of information to Authority

* 1. The Supplier must provide the Authority on request with:
     1. full details of the Protective Monitoring System it has implemented; and
     2. copies of monitoring logs and reports prepared as part of the Protective Monitoring System.

Changes to Protective Monitoring System

* 1. The Authority may at any time require the Supplier to update the Protective Monitoring System to:
     1. respond to a specific threat identified by the Authority;
     2. implement additional audit and monitoring requirements; and
     3. stream any specified event logs to the Authority's security information and event management system.

1. **Audit rights**

Right of audit

* 1. The Authority may undertake an audit of the Supplier or any Subcontractor to:
     1. verify the Supplier's or Subcontractor's (as applicable) compliance with the requirements of this Schedule 5 (*Security Management*) and the Data Protection Laws as they apply to Government Data;
     2. inspect the Supplier Information Management System (or any part of it);
     3. review the integrity, confidentiality and security of the Government Data; and/or
     4. review the integrity and security of the Code.
  2. Any audit undertaken under Paragraph 15.1:
     1. may only take place during the Term and for a period of 18 months afterwards; and
     2. is in addition to any other rights of audit the Authority has under this Contract.
  3. The Authority may not undertake more than one audit under Paragraph 15.1 in each calendar year unless the Authority has reasonable grounds for believing:
     1. the Supplier or any Subcontractor has not complied with its obligations under this Contract or the Data Protection Laws as they apply to the Government Data;
     2. there has been or is likely to be a Breach of Security affecting the Government Data or the Code; or
     3. where vulnerabilities, or potential vulnerabilities, in the Code have been identified by:
        1. an IT Health Check; or
        2. a Breach of Security.

Conduct of audits

* 1. The Authority must use reasonable endeavours to provide 15 Working Days' notice of an audit.
  2. The Authority must when conducting an audit:
     1. comply with all relevant policies and guidelines of the Supplier or Subcontractor (as applicable) concerning access to the Suppler Information Management System the Authority considers reasonable having regard to the purpose of the audit; and
     2. use reasonable endeavours to ensure that the conduct of the audit does not unreasonably disrupt the Supplier or Subcontractor (as applicable) or delay the provision of the Services.
  3. The Supplier must, and must ensure that Subcontractors, on demand provide the Authority with all co‑operation and assistance the Authority may reasonably require, including:
     1. all information requested by the Authority within the scope of the audit;
     2. access to the Supplier Information Management System; and
     3. access to the Supplier Personnel.

Response to audit findings

* 1. Where an audit finds that:
     1. the Supplier or a Subcontractor has not complied with this Contract or the Data Protection Laws as they apply to the Government Data; or
     2. there has been or is likely to be a Security Breach affecting the Government Data,
  2. the Authority may require the Supplier to remedy those defaults at its own cost and expense and within the time reasonably specified by the Authority.
  3. The exercise by the Authority of any rights it may have under this Paragraph 15 does not affect the exercise by it of any other or equivalent rights it may have under this Contract in respect of the audit findings.

1. **Breach of Security**

Reporting Breach of Security

* 1. If either party becomes aware of a Breach of Security it shall notify the other as soon as reasonably practicable after becoming aware of the breach, and in any event within [24] hours.

Immediate steps

* 1. The Supplier must, upon becoming aware of a Breach of Security immediately take those steps identified in the Security Management Plan and all other steps reasonably necessary to:
     1. minimise the extent of actual or potential harm caused by such Breach of Security;
     2. remedy such Breach of Security to the extent possible;
     3. apply a tested mitigation against any such Breach of Security; and
     4. prevent a further Breach of Security in the future which exploits the same root cause failure.

Subsequent action

* 1. As soon as reasonably practicable and, in any event, within 5 Working Days of the occurrence of the Breach of Security, or such other period specified by the Authority, provide to the Authority:
     1. full details of the Breach of Security; and
     2. if required by the Authority:
        1. a root cause analysis; and
        2. a draft plan addressing the Breach of Security

(a **Breach Action Plan**).

* 1. The draft Breach Action Plan must set out:
     1. in respect of each issue identified in the root cause analysis:
        1. how the issue will be remedied;
        2. the date by which the issue will be remedied; and
        3. the tests that the Supplier proposes to perform to confirm that the issue has been remedied or the finding addressed;
     2. the assistance the Supplier will provide to the Authority to resolve any impacts on the Authority, the Government Data and the Code;
     3. the Supplier's communication and engagement activities in respect of the Breach of Security, including any communication or engagement with individuals affected by any Breach of Security that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data; and
     4. the infrastructure, services and systems (including any contact centre facilities) the Supplier will establish to undertake the remediation, communication and engagement activities.
  2. The Supplier shall promptly provide the Authority with such technical and other information relating to the draft Breach Action Plan as the Authority requests.
  3. The Authority may:
     1. reject the draft Breach Action Plan where it considers that the draft Breach Action Plan is inadequate, providing its reasons for doing so, in which case:
        1. the Supplier shall within ten Working Days of the date on which the Authority rejected the draft Breach Action Plan, or such other period as the Authority requires, submit a revised draft Breach Action Plan that takes into account the Authority's reasons; and
        2. Paragraphs 16.5 and 16.6 shall apply to the revised draft Breach Action Plan; or
     2. accept the draft Breach Action Plan, in which case the Supplier must immediately start work on implementing the Breach Action Plan.
  4. When implementing the Breach Action Plan, the Supplier must:
     1. establish infrastructure, services and systems referred to in the Breach Action Plan;
     2. communicate and engage with affected individuals in accordance with the Breach Action Plan;
     3. communicate and engage with the Authority and stakeholders identified by the Authority in accordance with the Breach Plan and as otherwise required by the Authority;
     4. engage and deploy such additional resources as may be required to perform its responsibilities under the Breach Plan and this Contract in respect of the Personal Data Breach without any impact on the provision of the Services; and
     5. continue to implement the Breach Action Plan until the Authority indicates that the Breach of Security and the impacts on the Authority, the Government Data, the Code and the affected individuals have been resolved to the Authority's satisfaction.
  5. The obligation to provide and implement a Breach Action Plan under Paragraphs 16.3 to 16.7 continues notwithstanding the expiry or termination of this Contract.

Costs of preparing and implementing Breach Action Plan

* 1. The Supplier is solely responsible for its costs in preparing and implementing a Breach Action Plan.

Reporting of Breach of Security to regulator

* 1. Where the Law requires the Supplier report a Breach of Security to the appropriate regulator, the Supplier must:
     1. make that report within the time limits:
        1. specified by the relevant regulator; or
        2. otherwise required by Law; and
     2. to the extent that the relevant regulator or the Law permits, provide the Authority with a full, unredacted and unedited copy of that report at the same time it is sent to the relevant regulator.
  2. Where the Law requires the Authority to report a Breach of Security to the appropriate regulator, the Supplier must:
     1. provide such information and other input as the Authority requires within the timescales specified by the Authority; and
     2. ensure so far as practicable the report it sends to the relevant regulator is consistent with the report provided by the Authority.

1. **Exit management**
   1. In addition to any obligations on the Supplier under Schedule 21 (*Exit Management*) the Supplier must:
      1. agree with the Authority and, where required by the Supplier, the Replacement Supplier; and
      2. document as part of the Exit Plan,

a plan for the migration of the Government Data to the Authority and/or the Replacement Supplier (as required by the Authority) ("**Data Migration Plan**").

* 1. The Data Migration Plan must, at a minimum, include:
     1. the data formats of the Government Data;
     2. the roles and responsibilities of the Supplier, the Authority and (where applicable) the Replacement Supplier;
     3. the methods to be used to securely transfer the data;
     4. the timescales for the completion of all tasks and activities set out in the Data Migration Plan; and
     5. how data migration will be managed to ensure continuity of Services and the integrity, confidentiality and accessibility of the Government Data during that process.
  2. The Supplier shall comply with the provisions of the Data Migration Plan during Exit Management.

1. **Return and deletion of Government Data**
   1. The Supplier must create and maintain a register of:
      1. all Government Data the Supplier, or any Subcontractor, receives from or creates for the Authority; and
      2. those parts of the Supplier Information Management System, including those parts of the Supplier Information Management System that are operated or controlled by any Subcontractor, on which the Government Data is stored,

("**Government Data Register**").

* 1. The Supplier must:
     1. review and update the Government Data Register:
        1. within 10 Working Days of the Supplier or any Subcontractor changes those parts of the Supplier Information Management System on which the Government Data is stored;
        2. within 10 Working Days of a significant change in the volume, nature or overall sensitivity of the Government Data stored on the Supplier Information Management System;
        3. at least once every 12 months; and
     2. provide the Authority with a copy of the Government Data Register:
        1. whenever it updates the Government Data Register; and
        2. otherwise when the Authority requests.
  2. Subject to Paragraph 18.4, the Supplier must, and must ensure that all Subcontractors, securely erase any or all Government Data held by the Supplier or Subcontractor, including any or all Code:
     1. when requested to do so by the Authority; and
     2. using a deletion method agreed with the Authority that ensures that even a determined expert using specialist techniques can recover only a small fraction of the data deleted.
  3. Paragraph 18.4does not apply to Government Data:
     1. that is Personal Data in respect of which the Supplier is a Controller;
     2. to which the Supplier has rights to Handle independently from this Contract; or
     3. in respect of which, the Supplier is under an obligation imposed by Law to retain.
  4. The Supplier must, and must ensure that all Subcontractors, provide the Authority with copies of any or all Government Data held by the Supplier or Subcontractor, including any or all Code:
     1. when requested to do so by the Authority; and
     2. using the method specified by the Authority.

appendix 2 Security Requirements for Development

1. **Secure Software Development by Design**
   1. The Supplier must, and must ensure that all Subcontractors engaged in Development Activity, implement secure development and deployment practices to ensure that:
      1. no Malicious Software is introduced into the Developed System or the Supplier Information Management System; and
      2. the Developed System can continue to function in accordance with the Specification:
         1. in unforeseen circumstances; and
         2. notwithstanding any attack on the Developed System using common cyber‑attack techniques, including attacks using those vulnerabilities identified at any time in the OWASP Top Ten.
   2. To those ends, the Supplier must, and ensure that all Subcontractors engaged in Development Activity:
      1. comply with the Secure Development Guidance as if its requirements were terms of this Contract; and
      2. document the steps taken to comply with that guidance as part of the Security Management Plan.
   3. In particular, the Supplier must, and ensure that all Subcontractors engaged in Development Activity:
      1. ensure that all Supplier Personnel engaged in Development Activity are:
         1. trained and experienced in secure by design code development;
         2. provided with regular training in secure software development and deployment;
      2. ensure that all Code:
         1. is subject to a clear, well ‑organised, logical and documented architecture;
         2. follows OWASP Secure Coding Practice
         3. follows recognised secure coding standard, where one is available;
         4. employs consistent naming conventions;
         5. is coded in a consistent manner and style;
         6. is clearly and adequately documented to set out the function of each section of code;
         7. is subject to appropriate levels of review through automated and non‑automated methods both as part of:
            1. any original coding; and
            2. at any time the Code is changed; and
      3. ensure that all Development Environments:
         1. protect access credentials and secret keys;
         2. is logically separate from all other environments, including production systems, operated by the Supplier or Subcontractor;
         3. requires multi‑factor authentication to access;
         4. have onward technical controls to protect the Developed System or the Supplier Information Management System in the event a Development Environment is compromised; and
         5. use network architecture controls to constrain access from the Development Environment to the Developed System or the Supplier Information Management System.
2. **Secure Architecture**
   1. The Supplier shall design and build the Developed System in a manner consistent with:
      1. the NCSC's guidance on "Security Design Principles for Digital Services";
      2. where the Developed System will Handle bulk data, the NCSC's guidance on "Bulk Data Principles"; and
      3. the NCSC's guidance on "Cloud Security Principles".
   2. Where any of the documents referred to in Paragraph 2.1 provides for various options, the Supplier must document the option it has chosen to implement and its reasons for doing so.
   3. Notwithstanding anything in the specification for the Developed System or this Contract, the Supplier must ensure that the Developed System encrypts Government Data:
      1. when the Government Data is stored at any time when no operation is being performed on it; and
      2. when the Government Data is transmitted.
   4. The Supplier must ensure that the Developed System is developed and configured so as to provide for the matters set out in Paragraphs 13.1 to 13.4 of the Security Requirements.
3. **Code Repository and Deployment Pipeline**
4. The Supplier must, and must ensure that all Subcontractors engaged in Development Activity:
   1. when using a cloud ‑based code repository for the deployment pipeline, use only a cloud ‑based code repository that has been assessed against the NCSC Cloud Security Principles;
   2. ensure user access to code repositories is authenticated using credentials, with passwords or private keys;
   3. ensure secret credentials are separated from source code; and
   4. run automatic security testing as part of any deployment of the Developed System.
5. **Development and Testing Data**
6. The Supplier must, and must ensure that all Subcontractors engaged in Development Activity, use only anonymised, dummy or synthetic data when using data within the Development Environment for the purposes of development and testing.
7. **Code Reviews**
   1. The Supplier must:
      1. regularly; or
      2. as required by the Authority,
8. review the Code in accordance with the requirements of this Paragraph 5 ("**Code Review**").
   1. Before conducting any Code Review, the Supplier must agree with the Authority:
      1. the modules or elements of the Code subject to the Code Review;
      2. the development state at which the Code Review will take place;
      3. any specific security vulnerabilities the Code Review will assess; and
      4. the frequency of any Code Reviews,

(the "**Code Review Plan**").

* 1. For the avoidance of doubt the Code Review Plan may specify different modules or elements of the Code are reviewed at a different development state, for different security vulnerabilities and at different frequencies.
  2. The Supplier:
     1. must undertake Code Reviews in accordance with the Code Review Plan; and
     2. may undertake Code Reviews by automated means if this is consistent with the approach specified in the Code Review Plan.
  3. No later than ten Working Days or each Code Review, the Supplier must provide the Authority will a full, unedited and unredacted copy of the Code Review Report.
  4. Where the Code Review identifies any security vulnerabilities, the Supplier must:
     1. remedy these at its own cost and expense;
     2. ensure, so far as reasonably practicable, that the identified security vulnerabilities are not present in any other modules or code elements; and
     3. modify its approach to undertaking the Development Activities to ensure, so far as is practicable, the identified security vulnerabilities will not re‑occur; and
     4. provide the Authority with such information as it requests about the steps the Supplier takes under this Paragraph 5.6.

1. **Third-party Software**
2. The Supplier must not, and must ensure that Subcontractors do not, use any software to Handle Government Data where the licence terms of that software purport to grant the licensor rights to Handle the Government Data greater than those rights strictly necessary for the use of the software.
3. **Third-party Software Modules**
   1. Where the Supplier or a Subcontractor incorporates a Third-party Software Module into the Code, the Supplier must:
      1. verify the source and integrity of the Third-party Software Module by cryptographic signing or such other measure that provides the same level of assurance;
      2. perform adequate due diligence to determine whether there are any recognised security vulnerabilities with that Third-party Software Module;
      3. continue to monitor any such Third-party Software Module so as to ensure it promptly becomes aware of any newly ‑discovered security vulnerabilities; and
      4. take appropriate steps to minimise the effect of any such security vulnerability on the Developed System.
   2. For the purposes of Paragraph 7.1(b), the Supplier must perform due diligence that is proportionate to the significance of the Third-party Software Module within the Code.
   3. The Supplier must produce and maintain a register of all Third ‑party Software Modules that form part of the Code ("**Modules Register**").
   4. The Modules Register must include, in respect of each Third ‑party Software Module:
      1. full details of the developer of the module;
      2. the due diligence the Supplier undertook on the Third‑party Software Module before deciding to use it;
      3. any recognised security vulnerabilities in the Third‑party Software Module; and
      4. how the Supplier will minimise the effect of any such security vulnerability on the Developed System.
   5. The Supplier must:
      1. review and update the Modules Register:
         1. within [10] Working Days of becoming aware of a security vulnerability in any Third‑party Software Module; and
         2. at least once every 6 months; and
      2. provide the Authority with a copy of the Modules Register:
         1. whenever it updates the Modules Register; and
         2. otherwise when the Authority requests.

appendix 3 Security Working Group

1. **Role of the Security Working Group**
   1. The Security Working Group shall be responsible for the [insert remit of Security Working Group].
   2. The Security Working Group:
      1. monitors and provides recommendations to the Supplier on the [assurance] of the Supplier Information Management System;
      2. provides a forum for the sharing of information concerning security risks and threats and determining the appropriate mitigations;
      3. [insert remainder of terms of reference for Security Working Group].
2. **Meetings of the Security Working Group**
3. Paragraphs 3.4 to 3.7 of Schedule 17 (*Governance*) shall apply to the Security Working Group as if it were a Board established under that Schedule.
4. **Reports to the Security Working Group**
   1. The Supplier must provide the following reports no late than [5] Working Days before each meeting of the Security Woking Group:
      1. [insert list of required reports].
5. **Administration**
6. [The Supplier is responsible for the secretarial functions of the SWG.]

appendix 4 Subcontractor Security Requirements and Security Requirements for Development

* 1. The table below sets out the Security Requirements and Development Requirements that do **not** apply to particular categories of Subcontractors.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | * 1. SIMS Subcontractors | * 1. Higher-risk Subcontractors | * 1. Medium-risk Subcontractors | * 1. Subcontractors |
| * 1. Security Requirements that do not apply |  |  |  |  |
| * 1. Development Requirements that do not apply |  |  |  |  |

appendix 5 Security Management Plan Template

* 1. [**Insert EITHER Security Management Plan template OR link to Guidance including Security Management Plan template]**

appendix 6 Secure by Design Principles Evaluation Table

1. **Completion of Principles Evaluation Table**
   1. As part of the Security Management Plan, the Supplier must complete the table in this Appendix 6 (*Secure by Design Principles Evaluation Table*), unless that requirement is waived by the Authority.
   2. In completing this table, the Supplier must set out how it and any Subcontractors will meet the Secure by Design Principles.

| * 1. **Secure by Design Principle** | * 1. **Requirements** | * 1. **How the Supplier will meet the requirement** |
| --- | --- | --- |
| * 1. **Principle 1**   2. Create responsibility for cyber security risk   3. Assign a designated risk owner to be accountable for managing cyber security risks for the service within the contract. This must be a senior stakeholder with the experience, knowledge and authority to lead on security activities. | * 1. The Supplier designates a senior individual within their organisation who has overall accountability for ensuring the Secure by Design are met as part of the overall security requirements stated within the contract. |  |
| * 1. The Supplier designates a senior individual within the supplier delivery team - who will be reporting to the SRO, service owner or equivalent - with overall responsibility for the management of cyber security risks of digital services and technical infrastructure during their delivery. |  |
| * 1. The Supplier provides adequate and appropriately qualified resources to support the Authority with following the government [Secure by Design approach](https://www.security.gov.uk/guidance/secure-by-design/) as part of service delivery.   2. These resources must be reviewed at the beginning of each of the delivery phases during the delivery lifecycle of the service as agreed with the Authority. |  |
| * 1. **Principle 2**   2. Source secure technology products   3. Where third-party products are used, perform security due diligence by continually assessing platforms, software and code for security vulnerabilities. Mitigate risks and share findings with suppliers to help them improve product security. | * 1. The Supplier carries out proportionate (risk-driven) security reviews of third-party products before they are considered as a component of the digital service. The type and details of the review should be based on the significance associated with the product and are subject to agreement with the Authority. |  |
| * 1. The Supplier takes reasonable steps to reduce potential cyber security risks associated with using a third-party product as part of the service to a level that meets the Authority's security risk appetite for the service. Where the risk cannot be mitigated to such level, the Authority should be informed and asked to accept the risk associated with using the product. |  |
| * 1. The Supplier takes reasonable steps to assess third-party products used as a component of the digital service against legal and regulatory obligations and industry security standards specified by the Authority. Where the product doesn't meet the required obligations, the Supplier must discuss with the Authority the residual risks associated with using the product. |  |
| * 1. **Principle 3**   2. Adopt a risk-driven approach   3. Establish the project's risk appetite and maintain an assessment of cyber security risks to build protections appropriate to the evolving threat landscape. | * 1. As provided by the Authority, the Supplier should share the risk appetite across the supplier's delivery team from the outset. |  |
| * 1. The Supplier supports the Authority with identifying the cyber threats and attack paths as part of ongoing threat modelling during digital service delivery. |  |
| * 1. The Supplier supports the Authority with assessing cyber security risks and providing risk analysis details to help risk owners make informed risk decisions.   2. During the assessment, risks to the digital service are identified, analysed, prioritised, and appropriate mitigation is proposed taking into account the risk appetite during the lifecycle of the service. |  |
| * 1. The Supplier produces an output from the risk management process containing a clear set of security requirements that will reduce the risks in line with the agreed risk appetite and cyber security risk management approach. |  |
| * 1. The Supplier factors in the legal and regulatory requirements provided by the Authority in the risk management process and service design and build. |  |
| * 1. **Principle 4**   2. Design usable security controls   3. Perform regular user research and implement findings into service design to make sure security processes are fit for purpose and easy to understand. | * 1. The Supplier ensures that security requirements that are defined and documented as part of user research activities (for example user stories and user journeys) are fed into the design of the digital service. |  |
| * 1. The Supplier ensures that business objectives informing security requirements listed in the business case for the digital service are taken into consideration when designing security controls. |  |
| * 1. **Principle 5**   2. Build in detect and respond security   3. Design for the inevitability of security vulnerabilities and incidents. Integrate appropriate security logging, monitoring, alerting and response capabilities. These must be continually tested and iterated. | * 1. The Supplier responsible for building the digital service ensures that proportionate security logging, monitoring and alerting mechanisms able to discover cyber security events and vulnerabilities documented in the threat and risk assessment are designed into the service. |  |
| * 1. The Supplier responsible for building the digital service integrates incident response and recovery capabilities that are in line with the requirements and timescales documented in the service resilience or similar documentation. |  |
| * 1. The Supplier responsible for building the digital service regularly tests digital services and infrastructure to identify and fix weaknesses within systems. |  |
| * 1. **Principle 6**   2. Design flexible architectures   3. Implement digital services and update legacy components to allow for easier integration of new security controls in response to changes in business requirements, cyber threats and vulnerabilities. | * 1. As agreed with the Authority, the Supplier responsible for building the digital service uses flexible architectures and components that allow integration of new security measures in response to changes in business requirements, cyber threats and vulnerabilities. |  |
| * 1. The Supplier responsible for building the digital service tests security controls and verifying they are fit for purpose before deployment. |  |
| * 1. **Principle 7**   2. Minimise the attack surface   3. Use only the capabilities, software, data and hardware components necessary for a service to mitigate cyber security risks while achieving its intended use. | * 1. The Supplier responsible for building the digital service implements risk-driven security controls which meet the risk appetite and appropriate baseline as agreed with the Authority. |  |
| * 1. The Supplier responsible for building the digital service follows secure coding practices and, with consultation with the Authority's delivery team, identifies and mitigates vulnerabilities proactively reducing the number of vulnerabilities that potential attackers can exploit. |  |
| * 1. The Supplier retires service components (including data) securely when they are no longer needed, or at the end of their lifecycle. |  |
| * 1. **Principle 8**   2. Defend in depth   3. Create layered controls across a service so it's harder for attackers to fully compromise the system if a single control fails or is overcome. | * 1. The Supplier responsible for building the digital service adopts a defence in depth approach when designing the security architecture for the digital service. |  |
| * 1. The Supplier responsible for building the digital service implements security measures to incorporate segmentation. |  |

Schedule 6

Insurance Requirements

# Schedule 6: Insurance Requirements

1. Obligation to Maintain Insurances
   1. Without prejudice to its obligations to the Authority under this Contract, including its indemnity and liability obligations, the Supplier shall for the periods specified in this Schedule take out and maintain, or procure the taking out and maintenance of the insurances as set out in Annex 1 and any other insurances as may be required by applicable Law (together the “Insurances”). The Supplier shall ensure that each of the Insurances is effective no later than the date on which the relevant risk commences.
   2. The Insurances shall be maintained in accordance with Good Industry Practice and (so far as is reasonably practicable) on terms no less favourable than those generally available to a prudent contractor in respect of risks insured in the international insurance market from time to time.
   3. The Insurances shall be taken out and maintained with insurers who are:
      1. of good financial standing;
      2. appropriately regulated;
      3. regulated by the applicable regulatory body and is in good standing with that regulator; and
      4. except in the case of any Insurances provided by an Affiliate of the Supplier, of good repute in the international insurance market.
   4. The Supplier shall ensure that the public and products liability policy shall contain an indemnity to principals clause under which the Authority shall be indemnified in respect of claims made against the Authority in respect of death or bodily injury or third party property damage arising out of or in connection with the Contract and for which the Supplier is legally liable.
2. General Obligations
   1. Without limiting the other provisions of this Contract, the Supplier shall:
      1. take or procure the taking of all reasonable risk management and risk control measures in relation to the Services as it would be reasonable to expect of a prudent contractor acting in accordance with Good Industry Practice, including the investigation and reports of relevant claims to insurers;
      2. promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and
      3. hold all policies in respect of the Insurances and cause any insurance broker effecting the Insurances to hold any insurance slips and other evidence of placing cover representing any of the Insurances to which it is a party.
3. Failure to Insure
   1. The Supplier shall not take any action or fail to take any action or (insofar as is reasonably within its power) permit anything to occur in relation to it which would entitle any insurer to refuse to pay any claim under any of the Insurances.
   2. Where the Supplier has failed to purchase any of the Insurances or maintain any of the Insurances in full force and effect, the Authority may elect (but shall not be obliged) following written notice to the Supplier to purchase the relevant Insurances, and the Authority shall be entitled to recover the reasonable premium and other reasonable costs incurred in connection therewith as a debt due from the Supplier.
4. Evidence of Insurances
   1. The Supplier shall upon the Effective Date and within 15 Working Days after the renewal or replacement of each of the Insurances, provide evidence, in a form satisfactory to the Authority, that the Insurances are in force and effect and meet in full the requirements of this Schedule. Receipt of such evidence by the Authority shall not in itself constitute acceptance by the Authority or relieve the Supplier of any of its liabilities and obligations under this Contract.
5. Insurance for the Required Amount
   1. The Supplier shall ensure that any Insurances which are stated to have a minimum limit "in the aggregate" are maintained for the minimum limit of indemnity for the periods specified in this Schedule.
   2. Where the Supplier intends to claim under any of the Insurances for any matters that are not related to the Services and/or the Contract, where such claim is likely to result in the level of cover available under any of the Insurances being reduced below the minimum limit of indemnity specified in this Schedule, the Supplier shall promptly notify the Authority and provide details of its proposed solution for maintaining the minimum limit of indemnity specified in this Schedule.
6. Cancellation
   1. Subject to Paragraph 6.2, the Supplier shall notify the Authority in writing at least 5 Working Days prior to the cancellation, suspension, termination or non-renewal of any of the Insurances.
   2. Without prejudice to the Supplier’s obligations under Paragraph 4, Paragraph 6.2 shall not apply where the termination of any Insurances occurs purely as a result of a change of insurer in respect of any of the Insurances required to be taken out and maintained in accordance with this Schedule.
7. Insurance Claims, Premiums and Deductibles
   1. The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Services and/or this Contract for which it may be entitled to claim under any of the Insurances. In the event that the Authority receives a claim relating to or arising out of the Services and/or this Contract, the Supplier shall co-operate with the Authority and assist it in dealing with such claims at its own expense including without limitation providing information and documentation in a timely manner.
   2. The Supplier shall maintain a register of all claims under the Insurances in connection with this Contract and shall allow the Authority to review such register at any time.
   3. Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.
   4. Where any Insurance is subject to an excess or deductible below which the indemnity from insurers is excluded, the Supplier shall be liable for such excess or deductible. The Supplier shall not be entitled to recover from the Authority any sum paid by way of excess or deductible under the Insurances whether under the terms of this Contract or otherwise.

## Annex 1: Required Insurances

## Part A: Insurance Claim Notification

Except where the Authority is the claimant party, the Supplier shall give the Authority notice within 20 Working Days after any insurance claim in excess of [£100,000] relating to or arising out of the provision of the Services or this Contract on any of the Insurances or which, but for the application of the applicable policy excess, would be made on any of the Insurances and (if required by the Authority) full details of the incident giving rise to the claim.

***[Guidance: The insurance claims notification threshold should normally represent a significant or material value claim in connection with the requirement or represent an amount that would provide comfort to the Authority that it has knowledge of claims that might impact on the Authority.]***

## Part B: Third Party Public and Products Liability Insurance

1. Insured
   1. The Supplier
2. Interest
   1. To indemnify the Insured in respect of all sums which the Insured shall become legally liable to pay as damages, including claimant’s costs and expenses, in respect of accidental:
      1. death or bodily injury to or sickness, illness or disease contracted by any person; and
      2. loss of or damage to physical property;

happening during the period of insurance (as specified in Paragraph 5) and arising out of or in connection with the provision of the Services and in connection with this Contract.

1. Limit of indemnity
   1. Not less than £[to be determined by the Authority] in respect of any one occurrence, the number of occurrences being unlimited in any annual policy period, but £[to be determined by the Authority] in the aggregate per annum in respect of products and pollution liability.

*[Guidance:* ***The Authority should set the Limit of Indemnity by way of an insurable risk review (see MSC Guidance document). The level specified in the limit of indemnity above should be predicated upon:***

***The risk profile represented by the Contracting Authority requirement in question***

***Potential frequency and severity of claims and losses (not the value of the contract) relative to the risk exposure***

***Insurance market availability in prevailing insurance market conditions.***

*The wording on the limit of indemnity for third party public and products liability reflects what is available in UK insurance market conditions for this type of insurance only. While insurance is available in the UK on this basis, it may not be available in other parts of the world, in which case Suppliers may need to seek an alternative UK insurance policy on this basis*.]

1. Territorial limits

[United Kingdom]

*[Guidance:* ***The Authority should populate any additional territories relative to the service delivery. Annex 1 reflects United Kingdom insurance market conditions and availability only. Where there is an overseas insurance requirement consider obtaining professional insurance advice to set the appropriate requirement in Annex 1.]***

1. Period of insurance
   1. From the date of this Contract for the Term and renewable on an annual basis unless agreed otherwise by the Authority in writing.

*[Guidance:* ***The Authority should populate the period of insurance relative to the requirement in question. The period of insurance should reflect the period that the relevant insurable risk can materialise and take into account any contract specific issues such as phasing.]***

1. Cover features and extensions
   1. Indemnity to principals clause under which the Authority shall be indemnified in respect of claims made against the Authority in respect of death or bodily injury or third party property damage arising out of or in connection with the **Contract and for which the Supplier is legally liable**.

*[Guidance:* ***As part of the insurance review (see MSC Guidance document) the Authority should consider what additional cover features and extensions may be required to protect its interests (e.g. contractual liability extension and legal defence costs in addition to the limit of indemnity). The Authority may need to seek professional subject matter insurance advice in this regard.]***

1. Principal exclusions
   1. War and related perils.
   2. Nuclear and radioactive risks.
   3. Liability for death, illness, disease or bodily injury sustained by employees of the Insured arising out of the course of their employment.
   4. Liability arising out of the use of mechanically propelled vehicles whilst required to be compulsorily insured by applicable Law in respect of such vehicles.
   5. Liability in respect of predetermined penalties or liquidated damages imposed under any contract entered into by the Insured.
   6. Liability arising out of technical or professional advice other than in respect of death or bodily injury to persons or damage to third party property.
   7. Liability arising from the ownership, possession or use of any aircraft or marine vessel.
   8. Liability arising from seepage and pollution unless caused by a sudden, unintended and unexpected occurrence.

***[Guidance:******This list of exclusions represent insurance market wide exclusions for the third party public and products liability insurance. If something listed here is excluded and the Authority wishes it can be covered by an alternative insurance and included in Part D.]***

1. Maximum deductible threshold
   1. Not to exceed £[insert figure on contract award based on the Supplier’s acceptable response to the associated tender documents] for each and every third party property damage claim (personal injury claims to be paid in full).

## Part C: United Kingdom Compulsory Insurances

The Supplier shall meet its insurance obligations under applicable Law in full, including, UK employers’ liability insurance and motor third party liability insurance.

## Part D: Additional Insurances

***[Guidance:******The Authority may wish to consider including the following additional required insurances such as:***

|  |  |
| --- | --- |
| ***Professional Indemnity Insurance*** | ***Where the Authority requirement includes a potential breach of professional duty by the Supplier in connection with professional advice and /or professional services.*** |
| ***Property Damage Insurance / Goods in Transit Insurance*** | ***Where the Authority requirement necessitates primary perils insurance for relevant physical property (e.g. Authority physical property in the care, custody and control of the Supplier in delivering the Service).*** |
| ***Cyber Liability Insurance*** | ***Where the Authority requirement includes specific cyber risk exposures.*** |
| ***Environmental Liability Insurance or Contractors Pollution Liability Insurance*** | ***Where the Authority requirement includes exposure to significant pollution / contamination risks.*** |
| ***Aviation Insurances*** | ***Where the Authority requirement includes use of aircraft or activity airside.*** |
| ***Marine Insurances*** | ***Where the Authority requirement includes use of vessels or activity on water / sea.*** |
| ***Rail Insurances*** | ***Where the Authority requirement needs to adhere to the Office of Road and Rail insurance requirements.*** |

***The Authority should seek professional subject matter insurance advice to determine the scope, levels and drafting of any Additional Insurances.]***

Schedule 7

Authority Responsibilities

# Schedule 7: Authority Responsibilities

1. Introduction
   1. The responsibilities of the Authority set out in this Schedule shall constitute the Authority Responsibilities under this Contract. Any obligations of the Authority in Schedule 2 (*Services Description*) and Schedule 8 (*Supplier Solution*) shall not be Authority Responsibilities and the Authority shall have no obligation to perform any such obligations unless they are specifically stated to be “Authority Responsibilities” and cross referenced in the table in Paragraph 3.
   2. The responsibilities specified within this Schedule shall be provided to the Supplier free of charge, unless otherwise agreed between the Parties.
2. General Obligations
   1. The Authority shall:
      1. perform those obligations of the Authority which are set out in the Clauses of this Contract and the Paragraphs of the Schedules (except Schedule 2 (*Services Description*) and Schedule 8 (*Supplier Solution*));
      2. use its reasonable endeavours to provide the Supplier with access to appropriate members of the Authority’s staff, as such access is reasonably requested by the Supplier in order for the Supplier to discharge its obligations throughout the Term and the Termination Assistance Period;
      3. provide sufficient and suitably qualified staff to fulfil the Authority’s roles and duties under this Contract as defined in the Implementation Plan;
      4. use its reasonable endeavours to provide such documentation, data and/or other information that the Supplier reasonably requests that is necessary to perform its obligations under the terms of this Contract provided that such documentation, data and/or information is available to the Authority and is authorised for release by the Authority; and
      5. procure for the Supplier such agreed access and use of the Authority Premises (as a licensee only) and facilities (including relevant IT systems) as is reasonably required for the Supplier to comply with its obligations under this Contract, such access to be provided during the Authority’s normal working hours on each Working Day or as otherwise agreed by the Authority (such agreement not to be unreasonably withheld or delayed).
3. Specific Obligations
   1. The Authority shall, in relation to this Contract perform the Authority’s responsibilities identified as such in this Contract the details of which are set out below:

| **Document** | **Location (Paragraph)** |
| --- | --- |
| [Insert Schedule details here] | [Refer to specific Paragraphs here] |
|  |  |
|  |  |
|  |  |
|  |  |

Schedule 8

Supplier Solution

# Schedule 8: Supplier Solution

***[Guidance: Insert Supplier Solution here. Supplier Solution should include how the Supplier will deliver the Social Value requirements]***

Schedule 9

Implementation Plan

# Schedule 9: Implementation Plan

1. Introduction
   1. This Schedule:
      1. defines the process for the preparation and implementation of the Outline Implementation Plan and Detailed Implementation Plan; and
      2. identifies the Milestones (and associated Deliverables) including the Milestones which trigger payment to the Supplier of the applicable Milestone Payments following the issue of the applicable Milestone Achievement Certificate.
2. Outline Implementation Plan
   1. The Outline Implementation Plan is set out in Annex A.
   2. All changes to the Outline Implementation Plan shall be subject to the Change Control Procedure provided that the Supplier shall not attempt to postpone any of the Milestones using the Change Control Procedure or otherwise (except in accordance with Clause 29 (*Authority Cause*)).
3. Approval of the Detailed Implementation Plan
   1. The Supplier shall submit a draft of the Detailed Implementation Plan to the Authority for approval within 20 Working Days of the Effective Date.
   2. The Supplier shall ensure that the draft Detailed Implementation Plan:
      1. incorporates all of the Milestones and Milestone Dates set out in the Outline Implementation Plan;
      2. includes (as a minimum) the Supplier’s proposed timescales in respect of the following for each of the Milestones:
         1. the completion of each design document;
         2. the completion of the build phase;
         3. the completion of any Testing to be undertaken in accordance with Schedule 10 (*Testing Procedures*); and
         4. training and roll-out activities;
      3. clearly outlines all the steps required to implement the Milestones to be achieved in the next 15 months, together with a high level plan for the rest of the programme, in conformity with the Authority Requirements;
      4. clearly outlines the required roles and responsibilities of both Parties, including staffing requirements; and
      5. is produced using a software tool as specified, or agreed by the Authority.
   3. Prior to the submission of the draft Detailed Implementation Plan to the Authority in accordance with Paragraph 3.1, the Authority shall have the right:
      1. to review any documentation produced by the Supplier in relation to the development of the Detailed Implementation Plan, including:
         1. details of the Supplier’s intended approach to the Detailed Implementation Plan and its development;
         2. copies of any drafts of the Detailed Implementation Plan produced by the Supplier; and
         3. any other work in progress in relation to the Detailed Implementation Plan; and
      2. to require the Supplier to include any reasonable changes or provisions in the Detailed Implementation Plan.
   4. Following receipt of the draft Detailed Implementation Plan from the Supplier, the Authority shall:
      1. review and comment on the draft Detailed Implementation Plan as soon as reasonably practicable; and
      2. notify the Supplier in writing that it approves or rejects the draft Detailed Implementation Plan no later than 20 Working Days after the date on which the draft Detailed Implementation Plan is first delivered to the Authority.
   5. If the Authority rejects the draft Detailed Implementation Plan:
      1. the Authority shall inform the Supplier in writing of its reasons for its rejection; and
      2. the Supplier shall then revise the draft Detailed Implementation Plan (taking reasonable account of the Authority’s comments) and shall re-submit a revised draft Detailed Implementation Plan to the Authority for the Authority’s approval within 20 Working Days of the date of the Authority’s notice of rejection. The provisions of Paragraph 3.4 and this Paragraph 3.5 shall apply again to any resubmitted draft Detailed Implementation Plan, provided that either Party may refer any disputed matters for resolution by the Dispute Resolution Procedure at any time.
   6. If the Authority approves the draft Detailed Implementation Plan, it shall replace the Outline Implementation Plan from the date of the Authority’s notice of approval.
4. Updates to And Maintenance of the Detailed Implementation Plan
   1. Following the approval of the Detailed Implementation Plan by the Authority:
      1. the Supplier shall submit a revised Detailed Implementation Plan to the Authority every 3 months starting 3 months from the Effective Date;
      2. without prejudice to Paragraph 4.1.1, the Authority shall be entitled to request a revised Detailed Implementation Plan at any time by giving written notice to the Supplier and the Supplier shall submit a draft revised Detailed Implementation Plan to the Authority within 20 Working Days of receiving such a request from the Authority (or such longer period as the Parties may agree provided that any failure to agree such longer period shall be referred to the Dispute Resolution Procedure);
      3. any revised Detailed Implementation Plan shall (subject to Paragraph 4.2) be submitted by the Supplier for approval in accordance with the procedure set out in Paragraph 3; and
      4. the Supplier’s performance against the Implementation Plan shall be monitored at meetings of the Service Management Board (as defined in Schedule 17 (*Governance*). In preparation for such meetings, the current Detailed Implementation Plan shall be provided by the Supplier to the Authority not less than 5 Working Days in advance of each meeting of the Service Management Board.
   2. Save for any amendments which are of a type identified and notified by the Authority (at the Authority’s discretion) to the Supplier in writing as not requiring approval, any material amendments to the Detailed Implementation Plan shall be subject to the Change Control Procedure provided that:
      1. any amendments to elements of the Detailed Implementation Plan which are based on the contents of the Outline Implementation Plan shall be deemed to be material amendments; and
      2. in no circumstances shall the Supplier be entitled to alter or request an alteration to any Milestone Date except in accordance with Clause 29 (*Authority Cause*).
   3. Any proposed amendments to the Detailed Implementation Plan shall not come into force until they have been approved in writing by the Authority.
5. Government Reviews
   1. The Supplier acknowledges that the Services may be subject to Government review at key stages of the project. The Supplier shall cooperate with any bodies undertaking such review and shall allow for such reasonable assistance as may be required for this purpose within the Charges.

## Annex A: Outline Implementation Plan

| Milestone | Deliverables (bulleted list showing all Deliverables (and associated tasks) required for each Milestone) | Duration (Working Days) | Milestone Date | Authority Responsibilities (if applicable) | Link to ATP/CPP |
| --- | --- | --- | --- | --- | --- |
| Concept Design | [Statement of Requirements System/Application Specifications Interface Specifications Systems Testing Strategy Implementation Strategy and Plan Risk and Issues Management Plan Outline Disaster Recovery Plan Project Schedule Service Management Plan] |  |  |  |  |
| Full Development | [Design Verification Reports Design Validation Reports Change Management Plan System/Application Implementation Plan Risk and Issues Management Project Schedule Service Management Plan] |  |  |  |  |
| System User Testing | System Test Report Risk and Issues Management Plan Project Schedule  Service Management Plan Defects Log Final Inspection and Testing Report |  |  |  |  |
| User Readiness for Service | Training Plan Risk and Issues Log Implementation Plan Operations Plan Data Conversion & Cutover Plan Project Schedule Service Management Plan |  |  |  |  |
| Implementation | Implementation Plan Training Scripts |  |  |  |  |
| In Service Support | Post Implementation Report Data Conversion and Cut-Over Plan Service Delivery Reports Risk and Issues Log Service Management Plan Defects Log |  |  |  |  |

Schedule 10

Testing Procedures

# Schedule 10: Testing Procedures

1. Definitions
   1. In this Schedule, the following definitions shall apply:

|  |  |
| --- | --- |
| “Component” | any constituent parts of the infrastructure for a Service, hardware or Software; |
| “Material Test Issue” | a Test Issue of Severity Level 1 or Severity Level 2; |
| “Severity Level” | the level of severity of a Test Issue, the criteria for which are described in Annex 1; |
| “Test Certificate” | a certificate materially in the form of the document contained in Annex 2 issued by the Authority when a Deliverable has satisfied its relevant Test Success Criteria; |
| “Test Issue” | any variance or non-conformity of a Deliverable from its requirements (such requirements being set out in the relevant Test Success Criteria); |
| “Test Issue Threshold” | in relation to the Tests applicable to a Milestone, a maximum number of Severity Level 3, Severity Level 4 and Severity Level 5 Test Issues as set out in the relevant Test Plan; |
| “Test Issue Management Log” | a log for the recording of Test Issues as described further in Paragraph 9.1; |
| “Test Plan” | a plan:   1. for the Testing of Deliverables; and 2. setting out other agreed criteria related to the achievement of Milestones,   as described further in Paragraph 5; |
| “Test Reports” | the reports to be produced by the Supplier setting out the results of Tests; |
| “Test Specification” | the specification that sets out how Tests will demonstrate that the Test Success Criteria have been satisfied, as described in more detail in Paragraph 7; |
| “Test Strategy” | a strategy for the conduct of Testing as described further in Paragraph 4; |
| “Test Success Criteria” | in relation to a Test, the test success criteria for that Test as referred to in Paragraph 6; |
| “Test Witness” | any person appointed by the Authority pursuant to Paragraph 10.1; and |
| “Testing Procedures” | the applicable testing procedures and Test Success Criteria set out in this Schedule. |

1. Risk
   1. The issue of a Test Certificate, a Milestone Achievement Certificate and/or a conditional Milestone Achievement Certificate shall not:
      1. operate to transfer any risk that the relevant Deliverable or Milestone is complete or will meet and/or satisfy the Authority’s requirements for that Deliverable or Milestone; or
      2. affect the Authority’s right subsequently to reject:
         1. all or any element of the Deliverables to which a Test Certificate relates; or
         2. any Milestone to which the Milestone Achievement Certificate relates.
   2. Notwithstanding the issuing of any Milestone Achievement Certificate (including the Milestone Achievement Certificate in respect of Authority to Proceed), the Supplier shall remain solely responsible for ensuring that:
      1. the Supplier Solution as designed and developed is suitable for the delivery of the Services and meets the Authority Requirements;
      2. the Services are implemented in accordance with this Contract; and
      3. each Target Performance Level is met from the relevant Operational Service Commencement Date.
2. Testing Overview
   1. All Tests conducted by the Supplier shall be conducted in accordance with the Test Strategy, the Test Plans and the Test Specifications.
   2. The Supplier shall not submit any Deliverable for Testing:
      1. unless the Supplier is reasonably confident that it will satisfy the relevant Test Success Criteria;
      2. until the Authority has issued a Test Certificate in respect of any prior, dependant Deliverable(s); and
      3. until the Parties have agreed the Test Plan and the Test Specification relating to the relevant Deliverable(s).
   3. The Supplier shall use reasonable endeavours to submit each Deliverable for Testing or re-Testing by or before the date set out in the Implementation Plan for the commencement of Testing in respect of the relevant Deliverable.
   4. Prior to the issue of a Test Certificate, the Authority shall be entitled to review the relevant Test Reports and the Test Issue Management Log.
   5. Any Disputes between the Authority and the Supplier regarding Testing shall be referred to the Dispute Resolution Procedure using the Expedited Dispute Timetable.
3. Test Strategy
   1. The Supplier shall develop the final Test Strategy as soon as practicable after the Effective Date but in any case no later than 20 Working Days (or such other period as the Parties may agree in writing) after the Effective Date.
   2. The final Test Strategy shall include:
      1. an overview of how Testing will be conducted in accordance with the Implementation Plan;
      2. the process to be used to capture and record Test results and the categorisation of Test Issues;
      3. the method for mapping the expected Test results to the Test Success Criteria;
      4. the procedure to be followed if a Deliverable fails to satisfy the Test Success Criteria or produces unexpected results, including a procedure for the resolution of Test Issues;
      5. the procedure to be followed to sign off each Test;
      6. the process for the production and maintenance of Test Reports and reporting, including templates for the Test Reports and the Test Issue Management Log, and a sample plan for the resolution of Test Issues;
      7. the names and contact details of the Authority’s and the Supplier’s Test representatives;
      8. a high level identification of the resources required for Testing, including facilities, infrastructure, personnel and Authority and/or third party involvement in the conduct of the Tests;
      9. the technical environments required to support the Tests; and
      10. the procedure for managing the configuration of the Test environments.
4. Test Plans
   1. The Supplier shall develop Test Plans and submit these for the approval of the Authority as soon as practicable but in any case no later than 20 Working Days (or such other period as the Parties may agree in the Test Strategy or otherwise agree in writing) prior to the start date for the relevant Testing (as specified in the Implementation Plan).
   2. Each Test Plan shall include as a minimum:
      1. the relevant Test definition and the purpose of the Test, the Milestone to which it relates, the requirements being tested and, for each Test, the specific Test Success Criteria to be satisfied;
      2. a detailed procedure for the Tests to be carried out, including:
         1. the timetable for the Tests, including start and end dates;
         2. the Testing mechanism;
         3. dates and methods by which the Authority can inspect Test results or witness the Tests in order to establish that the Test Success Criteria have been met;
         4. the mechanism for ensuring the quality, completeness and relevance of the Tests;
         5. the format and an example of Test progress reports and the process with which the Authority accesses daily Test schedules;
         6. the process which the Authority will use to review Test Issues and the Supplier’s progress in resolving these in a timely basis;
         7. the Test schedule;
         8. the re-Test procedure, the timetable and the resources which would be required for re-Testing; and
      3. the process for escalating Test Issues from a re-test situation to the taking of specific remedial action to resolve the Test Issue.
   3. The Authority shall not unreasonably withhold or delay its approval of the Test Plans provided that the Supplier shall incorporate any reasonable requirements of the Authority in the Test Plans.
5. Test Success Criteria
   1. The Test Success Criteria for:
      1. each Test that must be Achieved for the Supplier to Achieve either the ATP Milestone or a CPP Milestone are set out in Annex 4; and
      2. all other Tests shall be agreed between the Parties as part of the relevant Test Plan pursuant to Paragraph 5.
6. Test Specification
   1. Following approval of a Test Plan, the Supplier shall develop the Test Specification for the relevant Deliverables as soon as reasonably practicable and in any event at least 10 Working Days (or such other period as the Parties may agree in the Test Strategy or otherwise agree in writing) prior to the start of the relevant Testing (as specified in the Implementation Plan).
   2. Each Test Specification shall include as a minimum:
      1. the specification of the Test data, including its source, scope, volume and management, a request (if applicable) for relevant Test data to be provided by the Authority and the extent to which it is equivalent to live operational data;
      2. a plan to make the resources available for Testing;
      3. Test scripts;
      4. Test pre-requisites and the mechanism for measuring them; and
      5. expected Test results, including:
         1. a mechanism to be used to capture and record Test results; and
         2. a method to process the Test results to establish their content.
7. Testing
   1. Before submitting any Deliverables for Testing the Supplier shall subject the relevant Deliverables to its own internal quality control measures.
   2. The Supplier shall manage the progress of Testing in accordance with the relevant Test Plan and shall carry out the Tests in accordance with the relevant Test Specification. Tests may be witnessed by the Test Witnesses in accordance with Paragraph 10.
   3. The Supplier shall notify the Authority at least 10 Working Days (or such other period as the Parties may agree in writing) in advance of the date, time and location of the relevant Tests and the Authority shall ensure that the Test Witnesses attend the Tests, except where the Authority has specified in writing that such attendance is not necessary.
   4. The Authority may raise and close Test Issues during the Test witnessing process.
   5. The Supplier shall provide to the Authority in relation to each Test:
      1. a draft Test Report not less than 2 Working Days (or such other period as the Parties may agree in writing) prior to the date on which the Test is planned to end; and
      2. the final Test Report within 5 Working Days (or such other period as the Parties may agree in writing) of completion of Testing.
   6. Each Test Report shall provide a full report on the Testing conducted in respect of the relevant Deliverables, including:
      1. an overview of the Testing conducted;
      2. identification of the relevant Test Success Criteria that have been satisfied;
      3. identification of the relevant Test Success Criteria that have not been satisfied together with the Supplier’s explanation of why those criteria have not been met;
      4. the Tests that were not completed together with the Supplier’s explanation of why those Tests were not completed;
      5. the Test Success Criteria that were satisfied, not satisfied or which were not tested, and any other relevant categories, in each case grouped by Severity Level in accordance with Paragraph 9.1; and
      6. the specification for any hardware and software used throughout Testing and any changes that were applied to that hardware and/or software during Testing.
8. Test Issues
   1. Where a Test Report identifies a Test Issue, the Parties shall agree the classification of the Test Issue using the criteria specified in Annex 1 and the Test Issue Management Log maintained by the Supplier shall log Test Issues reflecting the Severity Level allocated to each Test Issue.
   2. The Supplier shall be responsible for maintaining the Test Issue Management Log and for ensuring that its contents accurately represent the current status of each Test Issue at all relevant times. The Supplier shall make the Test Issue Management Log available to the Authority upon request.
   3. The Authority shall confirm the classification of any Test Issue unresolved at the end of a Test in consultation with the Supplier. If the Parties are unable to agree the classification of any unresolved Test Issue, the Dispute shall be dealt with in accordance with the Dispute Resolution Procedure using the Expedited Dispute Timetable.
9. Test Witnessing
   1. The Authority may, in its sole discretion, require the attendance at any Test of one or more Test Witnesses selected by the Authority, each of whom shall have appropriate skills to fulfil the role of a Test Witness.
   2. The Supplier shall give the Test Witnesses access to any documentation and Testing environments reasonably necessary and requested by the Test Witnesses to perform their role as a Test Witness in respect of the relevant Tests.
   3. The Test Witnesses:
      1. shall actively review the Test documentation;
      2. will attend and engage in the performance of the Tests on behalf of the Authority so as to enable the Authority to gain an informed view of whether a Test Issue may be closed or whether the relevant element of the Test should be re-Tested;
      3. shall not be involved in the execution of any Test;
      4. shall be required to verify that the Supplier conducted the Tests in accordance with the Test Success Criteria and the relevant Test Plan and Test Specification;
      5. may produce and deliver their own, independent reports on Testing, which may be used by the Authority to assess whether the Tests have been Achieved;
      6. may raise Test Issues on the Test Issue Management Log in respect of any Testing; and
      7. may require the Supplier to demonstrate the modifications made to any defective Deliverable before a Test Issue is closed.
10. Test Quality Audit
    1. Without prejudice to its rights pursuant to Clause 12.2.2 (*Records, Reports, Audits & Open Book Data*), the Authority may perform on-going quality audits in respect of any part of the Testing (each a “Testing Quality Audit”) subject to the provisions set out in the agreed Quality Plan.
    2. The focus of the Testing Quality Audits shall be on:
       1. adherence to an agreed methodology;
       2. adherence to the agreed Testing process;
       3. adherence to the Quality Plan;
       4. review of status and key development issues; and
       5. identification of key risk areas.
    3. The Supplier shall allow sufficient time in the Test Plan to ensure that adequate responses to a Testing Quality Audit can be provided.
    4. The Authority will give the Supplier at least 5 Working Days’ written notice of the Authority’s intention to undertake a Testing Quality Audit and the Supplier may request, following receipt of that notice, that any Testing Quality Audit be delayed by a reasonable time period if in the Supplier’s reasonable opinion, the carrying out of a Testing Quality Audit at the time specified by the Authority will materially and adversely impact the Implementation Plan.
    5. A Testing Quality Audit may involve document reviews, interviews with the Supplier Personnel involved in or monitoring the activities being undertaken pursuant to this Schedule, the Authority witnessing Tests and demonstrations of the Deliverables to the Authority. Any Testing Quality Audit shall be limited in duration to a maximum time to be agreed between the Supplier and the Authority on a case by case basis (such agreement not to be unreasonably withheld or delayed). The Supplier shall provide all reasonable necessary assistance and access to all relevant documentation required by the Authority to enable it to carry out the Testing Quality Audit.
    6. If the Testing Quality Audit gives the Authority concern in respect of the Testing Procedures or any Test, the Authority shall:
       1. discuss the outcome of the Testing Quality Audit with the Supplier, giving the Supplier the opportunity to provide feedback in relation to specific activities; and
       2. subsequently prepare a written report for the Supplier detailing its concerns,

and the Supplier shall, within a reasonable timeframe, respond in writing to the Authority’s report.

* 1. In the event of an inadequate response to the Authority’s report from the Supplier, the Authority (acting reasonably) may withhold a Test Certificate (and consequently delay the grant of a Milestone Achievement Certificate) until the issues in the report have been addressed to the reasonable satisfaction of the Authority.

1. Outcome of Testing
   1. The Authority shall issue a Test Certificate as soon as reasonably practicable when the Deliverables satisfy the Test Success Criteria in respect of that Test without any Test Issues.
   2. If the Deliverables (or any relevant part) do not satisfy the Test Success Criteria then the Authority shall notify the Supplier and:
      1. the Authority may issue a Test Certificate conditional upon the remediation of the Test Issues;
      2. where the Parties agree that there is sufficient time prior to the relevant Milestone Date, the Authority may extend the Test Plan by such reasonable period or periods as the Parties may reasonably agree and require the Supplier to rectify the cause of the Test Issue and re-submit the Deliverables (or the relevant part) to Testing; or
      3. where the failure to satisfy the Test Success Criteria results, or is likely to result, in the failure (in whole or in part) by the Supplier to meet a Milestone, then without prejudice to the Authority’s other rights and remedies, such failure shall constitute a Notifiable Default for the purposes of Clause 25.1 (*Rectification Plan Process*).
   3. The Authority shall be entitled, without prejudice to any other rights and remedies that it has under this Contract, to recover from the Supplier any reasonable additional costs it may incur as a direct result of further review or re-Testing which is required for the Test Success Criteria for that Deliverable to be satisfied.
2. Issue of Milestone Achievement Certificate
   1. The Authority shall issue a Milestone Achievement Certificate in respect of a given Milestone as soon as is reasonably practicable following:
      1. the issuing by the Authority of Test Certificates and/or conditional Test Certificates in respect of all Deliverables related to that Milestone which are due to be Tested; and
      2. performance by the Supplier to the reasonable satisfaction of the Authority of any other tasks identified in the Implementation Plan as associated with that Milestone (which may include the submission of a Deliverable that is not due to be Tested, such as the production of Documentation).
   2. The grant of a Milestone Achievement Certificate shall entitle the Supplier to the receipt of a payment in respect of that Milestone in accordance with the provisions of Schedule 11 (*Charges and Invoicing*).
   3. If a Milestone is not Achieved, the Authority shall promptly issue a report to the Supplier setting out:
      1. the applicable Test Issues ; and
      2. any other reasons for the relevant Milestone not being Achieved.
   4. If there are Test Issues but these do not exceed the Test Issues Threshold, then provided there are no Material Test Issues, the Authority shall issue a Milestone Achievement Certificate.
   5. Without prejudice to the Authority’s other remedies the following shall constitute a Notifiable Default for the purposes of Clause 25.1 (*Rectification Plan Process*) and the Authority shall refuse to issue a Milestone Achievement Certificate where:
      1. there is one or more Material Test Issue(s); or
      2. the information required under Schedule 20 (*Reports and Records Provisions*) (Annex 2: *Records To Upload To Virtual Library*) has not been uploaded to the Virtual Library in accordance with Paragraph 2 of that Schedule.
   6. If there are Test Issues which exceed the Test Issues Threshold but there are no Material Test Issues, the Authority may at its discretion (without waiving any rights in relation to the other options) choose to issue a Milestone Achievement Certificate conditional on the remediation of the Test Issues in accordance with an agreed Rectification Plan provided that:
      1. any Rectification Plan shall be agreed before the issue of a conditional Milestone Achievement Certificate unless the Authority agrees otherwise (in which case the Supplier shall submit a Rectification Plan for approval by the Authority within 10 Working Days of receipt of the Authority’s report pursuant to Paragraph 13.3); and
      2. where the Authority issues a conditional Milestone Achievement Certificate, it may (but shall not be obliged to) revise the failed Milestone Date and any subsequent Milestone Date.

## Annex 1: Test Issues – Severity Levels

1. Severity Levels
   1. **Severity Level 1 Test Issue:** a Test Issue that causes non-recoverable conditions, e.g. it is not possible to continue using a Component, a Component crashes, there is database or file corruption, or data loss;
   2. **Severity Level 2 Test Issue:** a Test Issue for which, as reasonably determined by the Authority, there is no practicable workaround available, and which:
      1. causes a Component to become unusable;
      2. causes a lack of functionality, or unexpected functionality, that has an impact on the current Test; or
      3. has an adverse impact on any other Component(s) or any other area of the Services;
   3. **Severity Level 3 Test Issue:** a Test Issue which:
      1. causes a Component to become unusable;
      2. causes a lack of functionality, or unexpected functionality, but which does not impact on the current Test; or
      3. has an impact on any other Component(s) or any other area of the Services;

but for which, as reasonably determined by the Authority, there is a practicable workaround available;

* 1. **Severity Level 4 Test Issue:** a Test Issue which causes incorrect functionality of a Component or process, but for which there is a simple, Component based, workaround, and which has no impact on the current Test, or other areas of the Services; and
  2. **Severity Level 5 Test Issue:** a Test Issue that causes a minor problem, for which no workaround is required, and which has no impact on the current Test, or other areas of the Services.

## Annex 2: Test Certificate

To: [Name of Supplier]

From: [Name of Authority]

[Date]

Dear Sirs,

TEST CERTIFICATE

Deliverables: **[insert** description of Deliverables]

We refer to the agreement (the “Contract”) relating to the provision of the Services between the [name of Authority] (the “Authority”) and [name of Supplier] (the “Supplier”) dated [date].

Capitalised terms used in this certificate have the meanings given to them in Schedule 1 (*Definitions*) or Schedule 10 (*Testing Procedures*) of the Contract.

[We confirm that the Deliverables listed above have been tested successfully in accordance with the Test Plan relevant to those Deliverables.]

OR

[This Test Certificate is issued pursuant to Paragraph 12.1 of Schedule 10 (*Testing Procedures*) of the Contract on the condition that any Test Issues are remedied in accordance with the Rectification Plan attached to this certificate.]\*

*\*delete as appropriate*

Yours faithfully

[Name]

[Position]

acting on behalf of [name of Authority]

## Annex 3: Milestone Achievement Certificate

To: [Name of Supplier]

From: [Name of Authority]

[Date]

Dear Sirs,

MILESTONE ACHIEVEMENT CERTIFICATE

Milestone: **[insert** description of Milestone]

We refer to the agreement (the “Contract”) relating to the provision of the Services between the [name of Authority] (the “Authority”) and [name of Supplier] (the “Supplier”) dated [date].

Capitalised terms used in this certificate have the meanings given to them in Schedule 1 (*Definitions*) or Schedule 10 (*Testing Procedures*) of the Contract.

[We confirm that all the Deliverables relating to Milestone [number] have been tested successfully in accordance with the Test Plan relevant to this Milestone [or that a conditional Test Certificate has been issued in respect of those Deliverables that have not satisfied the relevant Test Success Criteria.]]\*

OR

[This Milestone Achievement Certificate is granted pursuant to Paragraph 13.1 of Schedule 10 (*Testing Procedures*) of the Contract on the condition that any Test Issues are remedied in accordance with the Rectification Plan attached to this certificate.]\*

[You may now issue an invoice in respect of the Milestone Payment associated with this Milestone in accordance with the provisions of Schedule 11 (*Charges and Invoicing*)]\*

*\*delete as appropriate*

Yours faithfully

[Name]

[Position]

acting on behalf of [Authority]

## Annex 4: Test Success Criteria

1. Tests to be Achieved in order to Achieve the ATP Milestone

| **Test** | **Pre-conditions\*** | **Test Success Criteria** |
| --- | --- | --- |
| [List all Tests relating to ATP Milestone] |  |  |
|  |  |  |

\* Note: The Pre-Conditions are that e.g. the Success Criteria for the previous Tests must be satisfied before the ATP Milestone tests are commenced

1. Tests to be Achieved in order to Achieve a CPP Milestone

| **CPP Milestone Charge No.** | **Test** | **Test Success Criteria** |
| --- | --- | --- |
|  | [List all Tests relating to CPP Milestone Charge No.] |  |
|  |  |  |

Schedule 11

Charges and Invoicing

# Schedule 11: Charges and Invoicing

1. Definitions
   1. In this Schedule, the following definitions shall apply:

|  |  |
| --- | --- |
| “Achieved Profit Margin” | the cumulative Supplier Profit Margin calculated from (and including) the Effective Date (or, if applicable, the date of the last adjustment to the Charges made pursuant to Paragraph 2.2 of Part D) to (and including) the last day of the previous Contract Year; |
| “Anticipated Contract Life Profit Margin” | the anticipated Supplier Profit Margin over the Term as reflected in the Financial Model; |
| “Capped ADR” | in relation to a Milestone Payment or Service Charge means a capped average day rate calculated by reference to a Time and Materials pricing mechanism, £**[insert** amount]; |
| “Certificate of Costs” | a certificate of costs signed by the Supplier’s Chief Financial Officer or Director of Finance (or equivalent as agreed in writing by the Authority in advance of issue of the relevant certificate) and substantially in the format set out in Annex 3; |
| “Costs” | the following costs (without double recovery) to the extent that they are reasonably and properly incurred by the Supplier in providing the Services:   1. the cost to the Supplier or the Key Sub-contractor (as the context requires), calculated per Work Day, of engaging the Supplier Personnel, including:    1. base salary paid to the Supplier Personnel;    2. employer’s national insurance contributions;    3. Employer Pension Contributions;    4. car allowances;    5. any other contractual employment benefits;    6. staff training;    7. work place accommodation;    8. work place IT equipment and tools reasonably necessary to perform the Services (but not including items included within limb (b) below); and    9. reasonable recruitment costs, as agreed with the Authority; 2. costs incurred in respect of those Assets which are detailed on the Registers and which would be treated as capital costs according to generally accepted accounting principles within the UK, which shall include the cost to be charged in respect of Assets by the Supplier to the Authority or (to the extent that risk and title in any Asset is not held by the Supplier) any cost actually incurred by the Supplier in respect of those Assets; 3. operational costs which are not included within (a) or (b) above, to the extent that such costs are necessary and properly incurred by the Supplier in the delivery of the Services; 4. Forecast Contingency Costs; 5. Reimbursable Expenses to the extent these are incurred in delivering any Services where the Charges for those Services are to be calculated on a Fixed Price or Firm Price pricing mechanism;   but excluding:   * 1. Overhead;   2. financing or similar costs;   3. maintenance and support costs to the extent that these relate to maintenance and/or support services provided beyond the Term, whether in relation to Assets or otherwise;   4. taxation;   5. fines and penalties;   6. amounts payable under Schedule 13 (*Benchmarking*); and   7. non-cash items (including depreciation, amortisation, impairments and movements in provisions); |
| “Delay Payment Rate” | has the meaning given in Paragraph 1.1.1 of Part C; |
| “The Employer Pension Contributions” | means:   1. in respect of CSPS Eligible Employees those sums set out at clauses 7.1.1 (*annual administration charges covering core services*), 7.1.5 (*employer contributions*), 7.1.7 (*the ASLC*) and 7.1.8 (*flat charges applicable to the Partnership Pension Account*) of the Admission Agreement; 2. in respect of NHSPS Eligible Employees, the standard employer contribution rate applicable to NHS Pension Scheme employers during the Term and payable by the Supplier (but no other costs, contributions, charges or surcharges payable by the Supplier to or in respect of the NHS Pension Scheme or in respect of any NHS Premature Retirement Rights, unless otherwise agreed in writing by the Authority); 3. in respect of LGPS Eligible Employees the standard employer contribution rate applicable to LGPS Eligible Employees during the Term and payable by the Supplier (but no other costs, contributions, charges or surcharges payable by the Supplier to or in respect of the LGPS or in respect of any Beckmann Liabilities, unless otherwise agreed in writing by the Authority); and   such other employer pension contributions, charges or costs incurred by the Supplier which have been expressly agreed by the Authority in writing to constitute ‘Employer Pension Contributions’; |
| “Electronic Invoice Standard” | in relation to an electronic invoice means a form that:  (a) complies with the standard for electronic invoicing approved and issued by the British Standards Institution in the document numbered BS EN 16931-1:2017 (Electronic invoicing - Part 1: Semantic data model of the core elements of an electronic invoice); and  (b) uses a syntax which is listed as a syntax that complies with that standard in the document numbered PD CEN/TS 16931-2:2017 (Electronic invoicing - Part 2: List of syntaxes that comply with EN 16931-1) approved and issued by the British Standards Institution; |
| “Forecast Contingency Costs” | the costs which the Supplier forecasts may be incurred in relation to the risks and contingencies that are identified in the Risk Register, such costs being those set out in the column headed ‘Forecast Contingency Costs’ in the Risk Register (as such costs are updated from time to time); |
| “Guaranteed Maximum Price” | in relation to a Milestone, 110% of the Target Price for the relevant Milestone; |
| “Incurred Costs” | in relation to a Milestone, the sum of:   1. the fixed day costs set out in Table 3 of Annex 1 multiplied by the number of Work Days that have been expended by the Supplier Personnel in Achieving the relevant Milestone; and 2. any amount that would fall within limbs (b) or (c) of the definition of “Costs” (but subject to exceptions (i) to (vii) in that definition), to the extent that such amount has been incurred in Achieving the relevant Milestone; |
| “Indexation” and “Index” | the adjustment of an amount or sum in accordance with Paragraph 5 of Part C; |
| “Maximum Permitted Profit Margin” | the Anticipated Contract Life Profit Margin plus 5%; |
| “Milestone Group” | has the meaning given in Paragraph 1.4.3 of Part B; |
| “Milestone Retention” | has the meaning given in Paragraph 1.3 of Part B; |
| “Overhead” | those amounts which are intended to recover a proportion of the Supplier’s or the Key Sub-contractor’s (as the context requires) indirect corporate costs (including financing, marketing, advertising, research and development and insurance costs and any fines or penalties) but excluding allowable indirect costs apportioned to facilities and administration in the provision of Supplier Personnel and accordingly included within limb (a) of the definition of “Costs” or the day cost set out in Table 3 of Annex 1; |
| “Reimbursable Expenses” | reasonable out of pocket travel and subsistence (for example, hotel and food) expenses, properly and necessarily incurred in the performance of the Services, calculated at the rates and in accordance with the Authority’s expenses policy current from time to time, but not including:   1. travel expenses incurred as a result of Supplier Personnel travelling to and from their usual place of work, or to and from the premises at which the Services are principally to be performed, unless the Authority otherwise agrees in advance in writing; and 2. subsistence expenses incurred by Supplier Personnel whilst performing the Services at their usual place of work, or to and from the premises at which the Services are principally to be performed; |
| “Supplier Profit” | in relation to a period or a Milestone (as the context requires), the difference between the total Charges (in nominal cash flow terms but excluding any Deductions) and total Costs (in nominal cash flow terms) for the relevant period or in relation to the relevant Milestone; |
| “Supplier Profit Margin” | in relation to a period or a Milestone (as the context requires), the Supplier Profit for the relevant period or in relation to the relevant Milestone divided by the total Charges over the same period or in relation to the relevant Milestone and expressed as a percentage; |
| “Supporting Documentation” | sufficient information in writing to enable the Authority reasonably to assess whether the Charges, Reimbursable Expenses and other sums due from the Authority detailed in the information are properly payable, including copies of any applicable Milestone Achievement Certificates or receipts; |
| “Target Cost” | has the meaning given in Paragraph 3.1 of Part A; |
| “Target Price” | has the meaning given in Paragraph 3.1 of Part A; |
| “Verification Period” | in relation to an Allowable Assumption, the period from (and including) the Effective Date to (and including) the date at which the relevant Allowable Assumption expires, as set out against the relevant Allowable Assumption in column 11 in the table in Annex 5; |
| “Work Day” | 7.5 Work Hours, whether or not such hours are worked consecutively and whether or not they are worked on the same day; and |
| “Work Hours” | the hours spent by the Supplier Personnel properly working on the Services including time spent travelling (other than to and from the Supplier’s offices, or to and from the Sites) but excluding lunch breaks. |

## Part A: Pricing

1. Applicable Pricing Mechanism
   1. Milestone Payments and Service Charges shall be calculated using the pricing mechanism specified in Annex 2 and on the basis of the rates and prices specified in Annex 1 as more particularly set out in this Schedule.
   2. Table 1 of Annex 2 sets out which pricing mechanism shall be used to calculate each Milestone Payment, which shall be one or more of the following:
      1. “Time and Materials”, in which case the provisions of Paragraph 2 shall apply;
      2. “Guaranteed Maximum Price with Target Cost”, in which case the provisions of Paragraph 3 shall apply;
      3. “Fixed Price”, in which case the provisions of Paragraph 4 shall apply; or
      4. “Firm Price”, in which case the provisions of Paragraph 5 shall apply.
   3. Table 2 of Annex 2 sets out which pricing mechanism shall be used to calculate each Service Charge, which shall be one or more of the following:
      1. “Time and Materials”, in which case the provisions of Paragraph 2 shall apply;
      2. “Volume Based” pricing, in which case the provisions of Paragraph 6 shall apply; or
      3. “Fixed Price” in which case the provisions of Paragraph 4 shall apply.
2. Time and Materials Milestone Payments or Service Charges
   1. Where Table 1 or Table 2 of Annex 2 indicates that a Milestone Payment or Service Charge (as applicable) is to be calculated by reference to a Time and Materials pricing mechanism:
      1. the day rates set out in Table 1 of Annex 1 shall be used to calculate the relevant Charges, provided that the Supplier (or its Sub-contractor) shall:
         1. not be entitled to include any uplift for risks or contingencies within its day rates;
         2. not be paid any Charges to the extent that they would otherwise exceed the cap specified against the relevant Charge in Table 2 of Annex 1 unless the Supplier has obtained the Authority’s prior written consent. The Supplier shall monitor the amount of each Charge incurred in relation to the relevant cap and notify the Authority immediately in the event of any risk that the cap may be exceeded and the Authority shall instruct the Supplier on how to proceed;
         3. unless otherwise agreed by the Authority in relation to the relevant Milestone Payment or Service Charge (as the case may be), not be paid any Charges to the extent that they would otherwise exceed the amount calculated by multiplying:
            1. the total number of days expended by the Supplier in relation to the relevant Milestone; or
            2. the total number of days expended by the Supplier during the relevant Service Period in relation to the relevant Service,

by the Capped ADR; and

* + - 1. only be entitled to be paid Charges that have been properly and reasonably incurred, taking into account the Supplier’s obligation to deliver the Services in a proportionate and efficient manner; and
    1. the Supplier shall keep records of hours properly worked by Supplier Personnel (in the form of timesheets) and expenses incurred and submit a summary of the relevant records with each invoice. If the Authority requests copies of such records, the Supplier shall make them available to the Authority within 10 Working Days of the Authority’s request.
  1. The Supplier shall be entitled to Index the rates set out in Table 1 of Annex 1 and the Capped ADR in accordance with Paragraph 5 of Part C, but any caps set out in Table 2 of Annex 1 shall not be subject to Indexation.

1. Guaranteed Maximum Price with Target Cost Incentive Milestone Payments
   1. Where Table 1 of Annex 2 indicates that a Milestone Payment is to be calculated by reference to the Guaranteed Maximum Price with Target Cost pricing mechanism, the target Costs (the “Target Cost”) and the target Charge (the “Target Price”) for the relevant Milestone shall be as set out in Table 4 of Annex 1.
   2. If the Incurred Costs relating to a Milestone are lower than the Target Cost for that Milestone, the difference between the Incurred Costs and the Target Cost shall be shared equally between the Authority and the Supplier (resulting in the Supplier receiving a higher Supplier Profit Margin in relation to that Milestone), and the Milestone Payment shall be calculated as follows:

Milestone Payment = TP – ((TC – IC)/2)

where:

|  |  |
| --- | --- |
| TP | is the Target Price for the relevant Milestone; |
| TC | is the Target Cost for the relevant Milestone; and |
| IC | is the Incurred Costs relating to the relevant Milestone. |

* 1. If the Incurred Costs relating to a Milestone are greater than the Target Cost for that Milestone, the difference between the Incurred Costs and the Target Cost shall be borne equally between the Authority and the Supplier (resulting in the Supplier receiving a lower Supplier Profit Margin in relation to that Milestone), provided that the maximum Milestone Payment payable by the Authority for the relevant Milestone shall not exceed an amount equal to the guaranteed maximum price for that Milestone as set out in Table 4 of Annex 1 (the “Guaranteed Maximum Price”) Represented numerically:
     1. if:
        1. IC > TC; and
        2. TP + ((IC - TC)/2) < GMP,

then Milestone Payment = TP + ((IC - TC)/2); or

* + 1. if:
       1. IC > TC; and
       2. TP + ((IC - TC)/2) ≥ GMP,

then Milestone Payment = GMP

where:

|  |  |
| --- | --- |
| IC | is the Incurred Costs relating to the relevant Milestone; |
| TC | is the Target Cost for the relevant Milestone; |
| TP | is the Target Price for the relevant Milestone; and |
| GMP | is TP \* 1.1, being the Guaranteed Maximum Price for the relevant Milestone. |

* 1. The Supplier shall be entitled to Index the day costs set out in Table 3 of Annex 1 annually, but the Target Cost, Target Price and Guaranteed Maximum Price shall not be subject to Indexation.

1. Fixed Price Milestone Payments or Service Charges
   1. Where Table 1 or Table 2 of Annex 2 indicates that a Milestone Payment or Service Charge is to be calculated by reference to a Fixed Price pricing mechanism, the relevant Charge shall be the amount set out against that Charge in Table 5 of Annex 1.
   2. Charges calculated by reference to a Fixed Price pricing mechanism shall be subject to adjustment by way of Indexation.
2. Firm Price Milestone Payments
   1. Where Table 1 of Annex 2 indicates that a Milestone Payment is to be calculated by reference to a Firm Price pricing mechanism, the relevant Charge shall be the amount set out against that Charge in Table 6 of Annex 1.
   2. Charges calculated by reference to a Firm Price pricing mechanism shall not be subject to adjustment by way of Indexation.
3. Volume Based Service Charges
   1. Where Table 2 of Annex 2 indicates that a Service Charge is to be calculated by reference to a Volume Based pricing mechanism, the relevant Charges shall be calculated on the basis of the unit costs set out against that Service Charge in Table 7 of Annex 1.
   2. In the event that the volume of any Services that are to be calculated by reference to a Volume Based pricing mechanism fall outside the relevant volume bands set out against that Service Charge in Table 7 of Annex 1, the relevant Service Charges shall be calculated in accordance with the Change Control Procedure and Paragraph 4 of Part C.
   3. The Charge per unit set out in Table 7 of Annex 1 shall be subject to annual Indexation.
4. Reimbursable Expenses
   1. Where:
      1. Services are to be charged using the Time and Materials or Guaranteed Maximum Price with Target Cost pricing mechanism; and
      2. the Authority so agrees in writing,

the Supplier shall be entitled to be reimbursed by the Authority for Reimbursable Expenses (in addition to being paid the relevant Charges), provided that such Reimbursable Expenses are supported by Supporting Documentation.

* 1. The Authority shall provide a copy of its current expenses policy to the Supplier upon request.
  2. Except as expressly set out in Paragraph 7.1, the Charges shall include all costs and expenses relating to the Deliverables, the Services and/or the Supplier’s performance of its obligations under this Contract and no further amounts shall be payable by the Authority to the Supplier in respect of such performance, including in respect of matters such as:
     1. any incidental expenses that the Supplier incurs, including travel, subsistence and lodging, document and report reproduction, shipping, desktop and office equipment costs required by the Supplier Personnel, including network or data interchange costs or other telecommunications charges; or
     2. any amount for any services provided or costs incurred by the Supplier prior to the Effective Date.

## Part B: Charging Mechanisms

1. Milestone Payments
   1. Subject to the provisions of Paragraph 1.4 of Part C in relation to the deduction of Delay Payments, on the Achievement of a Milestone the Supplier shall be entitled to invoice the Authority for the Milestone Payment associated with that Milestone less the applicable Milestone Retention in accordance with this Part B.
   2. Each invoice relating to a Milestone Payment shall be supported by:
      1. a Milestone Achievement Certificate; and
      2. where the Milestone Payment is to be calculated by reference to a Guaranteed Maximum Price with Target Cost or Time and Materials pricing mechanism, a Certificate of Costs with Supporting Documentation.
   3. The “Milestone Retention” for each Milestone shall be calculated as follows:
      1. where the Milestone Payment for the relevant Milestone is determined by reference to a Guaranteed Maximum Price with Target Cost pricing mechanism, 10% of the Target Price for the Milestone;
      2. where the Milestone Payment for the relevant Milestone is determined by reference to a Time and Materials, Fixed Price or Firm Price pricing mechanism, 10% of the Charges for that Milestone,

and, in the case of a Key Milestone, prior to deduction from the Milestone Payment of any Delay Payment attributable to that Key Milestone.

Guaranteed Maximum Price with Target Cost pricing mechanism

* 1. Where a Milestone Payment relating to a single Milestone is to be calculated by reference to a Guaranteed Maximum Price with Target Cost pricing mechanism, then the following payment process shall apply:
     1. upon the issue of a Milestone Achievement Certificate for the Milestone, the Supplier may invoice the Authority for the Target Price for the relevant Milestone, less the Milestone Retention calculated using such Target Price; and
     2. no later than 60 Working Days after the invoice referred to in Paragraph 1.3.1 has been issued, the Supplier shall:
        1. submit to the Authority a report setting out the Incurred Costs and actual Milestone Payment for the Milestone;
        2. issue to the Authority an invoice or credit note for the difference between the actual Milestone Payment payable and the Target Price invoiced for the Milestone (in each case, after deducting the applicable Milestone Retention);
        3. where a credit note is to be issued to the Authority pursuant to Paragraph 1.4.2(b), repay to the Authority a sum equal to such difference as a debt within 10 Working Days of issue of the credit note; and
        4. issue a Certificate of Costs with Supporting Documentation, which shall exclude any accruals, prepayments and provisions.
     3. Where Milestones are stated in Table 4 of Annex 1 to constitute a group of Milestones (a “Milestone Group”) and the Milestone Payments relating to the Milestones in that Milestone Group are each to be calculated by reference to a Guaranteed Maximum Price with Target Cost pricing mechanism, then the following payment process shall apply:
     4. in respect of each Milestone within the Milestone Group, the Supplier may invoice the Authority for the Target Price for the relevant Milestone, less the Milestone Retention calculated using such Target Price, upon the issue of the associated Milestone Achievement Certificate; and
     5. no later than 60 Working Days after the issue of the invoice for the final Milestone Payment relating to the Milestone Group, the Supplier shall:
        1. submit to the Authority a report setting out the Incurred Costs and actual Milestone Payments for the Milestone Group;
        2. issue to the Authority an invoice or credit note for the difference between the aggregate of the actual Milestone Payments payable and Target Prices invoiced for Milestones in the Milestone Group (in each case, after deducting all Milestone Retentions relating to that Milestone Group);
        3. where a credit note is to be issued to the Authority pursuant to Paragraph 1.4.5(b), repay to the Authority a sum equal to such difference as a debt within 10 Working Days of issue of the credit note; and
        4. issue a Certificate of Costs with Supporting Documentation, which shall exclude any accruals, prepayments and provisions.
  2. If the Supplier does not repay any such sum as is referred to in Paragraph 1.4.2(b) or 1.4.5(b) within 10 Working Days of issue of the relevant credit note, it shall repay such sum together with interest on such sum at the applicable rate under the Late Payment of Commercial Debts (Interest) Act 1998, accruing on a daily basis from (and including) the due date up to (but excluding) the date of actual payment, whether before or after judgment.
  3. Following the issue of a Certificate of Costs in accordance with Paragraph 1.2, 1.4.2(c) or 1.4.5(c), the Supplier shall not be entitled to invoice the Authority for any additional Charges relating to the Milestone or Milestone Group (as applicable) save as provided in Paragraph 1.7.

Release of Milestone Retentions

* 1. On Achievement of a CPP Milestone relating to the Supplier Solution or one or more Services (as the case may be), the Supplier shall be entitled to invoice the Authority for an amount equal to all Milestone Retentions that relate to Milestones identified in the *“CPP Milestone Charge Number”* column of Table 1 (or, in relation to Milestone Retentions in respect of Optional Services, Table 4) of Annex 2 and corresponding CPP Milestone Charge Number identified in Table 2 of Annex 4 of Schedule 10 (*Testing Procedures*) as being payable in respect of that CPP Milestone and have not been paid before such CPP Milestone.

1. Service Charges
   1. Each Service to which a Service Charge relates shall commence on the Achievement of the Milestone set out against that Service in the “*Service* *Charge Trigger Event*” column of Table 2 of Annex 2.
   2. Service Charges shall be invoiced by the Supplier for each Service Period in arrear in accordance with the requirements of Part E.
   3. If a Service Charge is to be calculated by reference to a Fixed Price pricing mechanism and the relevant Service:
      1. commences on a day other than the first day of a month; and/or
      2. ends on a day other than the last day of a month,

the Service Charge for the relevant Service Period shall be pro-rated based on the proportion which the number of days in the month for which the Service is provided bears to the total number of days in that month.

* 1. Any Service Credits that accrue during a Service Period shall be deducted from the Service Charges payable for the next following Service Period. An invoice for a Service Charge shall not be payable by the Authority unless all adjustments (including Service Credits) relating to the Service Charges for the immediately preceding Service Period have been agreed.

1. Optional Services
   1. If the Authority gives notice pursuant to Clause 5.10 (*Optional Services*) that it requires the Supplier to provide any or all of the Optional Services:
      1. the Milestone Payments (if any) for the relevant Optional Services shall be calculated by reference to the pricing mechanism for those Optional Services set out in Table 3 of Annex 2; and
      2. the Service Charges for the relevant Optional Services shall be calculated by reference to the pricing mechanism for those Optional Services set out in Table 4 of Annex 2,

in both cases using the relevant rates and prices specified in Annex 1.

## Part C: Adjustments To The Charges And Risk Register

1. Delay Payments
   1. If a Key Milestone has not been Achieved on or before the relevant Milestone Date, the Supplier shall pay a Delay Payment to the Authority in respect of that Key Milestone. Delay Payments shall accrue:
      1. at the daily rate (the “Delay Payment Rate”) determined in accordance with Paragraph 1.2;
      2. from (but excluding) the relevant Milestone Date to (and including) the earlier of:
         1. the date on which the Key Milestone is Achieved; and
         2. the expiry of the Delay Deduction Period; and
      3. on a daily basis, with any part day’s Delay counting as a day.
   2. Where a Delay Payment is payable in respect of a Key Milestone, the Delay Payment Rate shall be:
      1. where the Supplier has given the Authority less than 3 months’ prior notice of the Delay, the amount set out in column 4 of Table 1 of Annex 2 for the Key Milestone;
      2. where the Supplier has given the Authority between three (3) months’ and six (6) months’ prior notice of the Delay, the amount set out in column 5 of Table 1 of Annex 2 for the Key Milestone; or
      3. where the Supplier has given the Authority more than 6 months’ prior notice of the Delay, the amount set out in column 6 of Table 1 of Annex 2 for the Key Milestone. The Supplier acknowledges and agrees that any Delay Payment is a price adjustment and not an estimate of the Loss that may be suffered by the Authority as a result of the Supplier's failure to Achieve the corresponding Milestone.
   3. The Delay Payment in respect of a Key Milestone shall be shown as a deduction from the amount due from the Authority to the Supplier in the next invoice due to be issued by the Supplier after the date on which the relevant Key Milestone is Achieved or the expiry of the Delay Deduction Period (as the case may be). If the relevant Key Milestone is not Achieved by the expiry of the Delay Deduction Period and no invoice is due to be issued by the Supplier within 10 Working Days of expiry of the Delay Deduction Period, then the Supplier shall within 10 Working Days of expiry of the Delay Deduction Period:
      1. issue a credit note to the Authority in respect of the total amount of the Delay Payment in respect of the Key Milestone for use by the Authority for accounting purposes; and
      2. pay to the Authority as a debt a sum equal to the total amount of the Delay Payment in respect of the Key Milestone together with interest on such amount at the applicable rate under the Late Payment of Commercial Debts (Interest) Act 1998, accruing on a daily basis from (and including) the due date up to (but excluding) the date of actual payment, whether before or after judgment.
2. Payments for Delays due to Authority Cause
   1. If the Supplier is entitled in accordance with Clause 29.1(c)(iv) (*Authority* *Cause*) to compensation for failure to Achieve a Milestone by its Milestone Date, then, subject always to Clause 23 (*Limitations on Liability*), such compensation shall be determined in accordance with the following principles:
      1. the compensation shall reimburse the Supplier for additional Costs incurred by the Supplier that the Supplier:
         1. can demonstrate it has incurred solely and directly as a result of the Authority Cause; and
         2. is, has been, or will be unable to mitigate, having complied with its obligations under Clause 29.1 (*Authority Cause*)

together with an amount equal to the Anticipated Contract Life Profit Margin thereon;

* + 1. the compensation shall not operate so as to put the Supplier in a better position than it would have been in but for the occurrence of the Authority Cause;
    2. where the Milestone Payment for the relevant Milestone is to be calculated by reference to the Guaranteed Maximum Price with Target Cost pricing mechanism, then:
       1. the Target Price for the Milestone shall be increased in accordance with the following formula:

where:

|  |  |
| --- | --- |
| NTP | is the revised Target Price for the relevant Milestone; |
| TP | is the original Target Price for the relevant Milestone; |
| AC | is an amount equal to any additional Costs incurred by the Supplier in Achieving the Milestone to the extent that the Supplier can demonstrate that such additional Costs were caused by the Authority Cause; and |
| x | is the Supplier Profit Margin that the Supplier would have received in respect of the relevant Milestone on the basis of the unadjusted Target Cost and unadjusted Target Price for that Milestone, as set out in Table 4 of Annex 1, expressed as a decimal; and |

* + - 1. the Guaranteed Maximum Price shall be increased to an amount equal to 110% of the Target Price as adjusted pursuant to Paragraph 2.1.3(a);
    1. where the relevant Milestone Payment is to be calculated based upon a Fixed Price or a Firm Price pricing mechanism, the compensation shall include such amount as is appropriate to maintain the Supplier Profit Margin set out in respect of the relevant Milestone in Table 5 or Table 6 of Annex 1; and
    2. where the Milestone Payment includes any Charges which are capped, then to the extent that the compensation agreed pursuant to this Paragraph 2 results in the Authority paying additional Time and Materials Charges for resources or effort which the Supplier demonstrates are required as a result of the Authority Cause, such additional Time and Materials Charges shall be disregarded for the purposes of calculating the relevant cap.
  1. The Supplier shall provide the Authority with any information the Authority may require in order to assess the validity of the Supplier’s claim to compensation.

1. Service Credits
   1. Service Credits shall be calculated by reference to the number of Service Points accrued in any one Service Period pursuant to the provisions of Schedule 3 (Performance Levels).
   2. For each Service Period:
      1. the Service Points accrued shall be converted to a percentage deduction from the Service Charges for the relevant Service Period on the basis of one point equating to a **[Insert** percentage]% deduction in the Service Charges; and
      2. the total Service Credits applicable for the Service Period shall be calculated in accordance with the following formula:

where:

|  |  |
| --- | --- |
| SC | is the total Service Credits for the relevant Service Period; |
| TSP | is the total Service Points that have accrued for the relevant Service Period; |
| X | is **[Insert** percentage deduction per Service Point]%; and |
| AC | is the total Services Charges payable for the relevant Service Period (prior to deduction of applicable Service Credits). |

* 1. The liability of the Supplier in respect of Service Credits shall be subject to Clause 23.4.3 (*Financial and other Limits*) provided that, for the avoidance of doubt, the operation of the Service Credit Cap shall not affect the continued accrual of Service Points in excess of such financial limit in accordance with the provisions of Schedule 3 (*Performance Levels*).
  2. Service Credits are a reduction of the Service Charges payable in respect of the relevant Services to reflect the reduced value of the Services actually received and are stated exclusive of VAT.
  3. Service Credits shall be shown as a deduction from the amount due from the Authority to the Supplier in the invoice for the Service Period immediately succeeding the Service Period to which they relate.

1. Changes to Charges
   1. Any Changes to the Charges shall be developed and agreed by the Parties in accordance with Schedule 18 (*Change Control Procedure*) and on the basis that the Supplier Profit Margin on such Charges shall:
      1. be no greater than that applying to Charges using the same pricing mechanism as at the Effective Date (as set out in the Contract Inception Report); and
      2. in no event exceed the Maximum Permitted Profit Margin.
   2. The Authority may request that any Impact Assessment presents Charges without Indexation for the purposes of comparison.
2. Indexation

*[Guidance: see paragraph 4.4 of the MSC Guidance document for further guidance regarding indexation.]*

* 1. Any amounts or sums in this Contract which are expressed to be “subject to Indexation” shall be adjusted in accordance with the provisions of this Paragraph 5 to reflect the effects of inflation.
  2. The following costs, expenses, fees or charges included in the Charges shall not be subject to adjustment under this Paragraph 5 and shall not be included in the relevant amount or sum for the purposes of Paragraph 5.3:
     1. Any costs charged by the Supplier to the Authority in respect of Assets or Authority Assets (including capital costs and installation, maintenance and support costs) which are incurred by the Supplier prior to the relevant adjustment date but which remain to be recovered through the Charges.
  3. Notwithstanding any other provisions of this Schedule, amounts or sums in this Contract shall not be subject to Indexation during the first [**Insert**: number] years following the Operational Service Commencement Date (the “**Non-Indexation Period**”).
  4. Where any amount or sum in this Contract is stated to be “subject to Indexation” then it will be indexed on the date which is one year after the end of the Non-Indexation Period to reflect the percentage change in the [**Insert:** name of appropriate price index (or indices) published by the Office of National Statistics or other reputable source] during that one year period immediately following the end of the Non-Indexation Period. Subsequent adjustments shall take place on each following yearly anniversary to reflect the percentage change in the price index since the previous change.
  5. Except as set out in this Paragraph 5, neither the Charges nor any other costs, expenses, fees or charges shall be adjusted to take account of any inflation, change to exchange rate, change to interest rate or any other factor or element which might otherwise increase the cost to the Supplier or Sub-contractors of the performance of their obligations.
  6. Where the price index referred to in Paragraph 5.4:
     1. used to carry out an indexation calculation is updated (for example due to it being provisional) then the indexation calculation shall also be updated unless the Authority and the Supplier agree otherwise; or
     2. is no longer published, the Authority and the Supplier shall agree an appropriate replacement index which shall cover to the maximum extent possible the same economic activities as the original index.

1. Allowable Assumptions
   1. The Supplier shall determine whether each Allowable Assumption is accurate within its Verification Period.
   2. During each Verification Period, the Authority shall provide the Supplier with reasonable assistance and access to information within its possession or reasonable control and which the Authority deems is relevant to the Allowable Assumption being verified.
   3. Within 10 Working Days of the end of each Verification Period, the Supplier shall provide the Authority with a written report setting out the results of the Supplier’s verification activity for the relevant Allowable Assumption, including whether the Allowable Assumption is accurate or whether the Implementation Plan and/or the Contract Inception Report require adjustment.
   4. Each Allowable Assumption shall be deemed accurate unless adjusting for the relevant Allowable Assumption has an impact:
      1. on the Financial Model greater than the associated trigger for invocation, as set out in column 9 of the table in Annex 5; or
      2. on the Implementation Plan which would require adjustment under the Change Control Procedure, as identified in column 3 of the table in Annex 5,

in which case Paragraph 6.5 shall apply.

* 1. Where the Parties agree that an Allowable Assumption is not accurate and the Financial Model and/or Implementation Plan require adjusting:
     1. the Supplier shall take all reasonable steps to mitigate the impact of the Allowable Assumption on the Financial Model and/or the Implementation Plan;
     2. the Supplier may (subject to Paragraph 6.5.3) propose a Change to take account of the impact of the adjustment of the Allowable Assumption and such Change Request shall be considered in accordance with the Change Control Procedure; and
     3. where the Supplier proposes a Change to the Charges under Paragraph 6.5.2, the Change Request shall reflect the requirements of the table in Annex 5, including the requirement that any proposed adjustment to the Charges shall not exceed the maximum impact on the relevant Charges as specified in column 7 of the table in Annex 5.

1. Risk Register
   1. The Parties shall review the Risk Register set out in Annex 4 from time to time and as otherwise required for the purposes of Schedule 17 (*Governance*).

## Part D: Excessive Supplier Profit Margin

1. Limit on Supplier Profit Margin
   1. The Supplier acknowledges that the Achieved Profit Margin applicable over the Term shall not exceed the Maximum Permitted Profit Margin.
   2. The Supplier shall include in each Annual Contract Report the Achieved Profit Margin as at the end of the Contract Year to which the Annual Contract Report is made up and the provisions of Paragraph 2 of Part B of Schedule 15 (*Financial Reports and Audit Rights*) shall apply to the approval of the Annual Contract Report.
2. Adjustment to the Charges in the Event of Excess Supplier Profit
   1. If an Annual Contract Report demonstrates (or it is otherwise determined pursuant to Paragraph 2 of Part B of Schedule 15 (*Financial Reports and Audit Rights*)) that the Achieved Profit Margin as at the end of the Contract Year to which the Annual Contract Report is made up exceeds the Maximum Permitted Profit Margin:
      1. the Supplier shall, within 5 Working Days of delivery to the Authority of the Annual Contract Report, propose such adjustments to the Charges as will ensure that the Achieved Profit Margin both over the Contract Year to which the next Annual Contract Report will relate and over the Term will not exceed the Maximum Permitted Profit Margin;
      2. the Authority (acting reasonably) may agree or reject the proposed adjustments;
      3. if the Authority rejects the proposed adjustments it shall give reasons and the Supplier shall propose revised adjustments within 10 Working Days of receiving those reasons; and
      4. if the Parties cannot agree such revised adjustments and the Authority terminates this Contract by issuing a Termination Notice to the Supplier pursuant to Clause 31.1.1 (*Termination by the* *Authority*), then for the purpose of calculating any Compensation Payment due to the Supplier, the Termination Notice shall be deemed to have been served as at the date of receipt by the Authority of the relevant Annual Contract Report.
   2. Pending agreement of a proposed adjustment to the Charges pursuant to this Part D, the Charges then in force shall continue to apply. Once the adjustments to the Charges are agreed in accordance with Paragraph 2.1, the Parties shall document the adjustment in a Change Authorisation Note and the adjusted Charges shall apply with effect from the first day of the Service Period that immediately follows the Service Period in which the Change Authorisation Note is executed or such other date as is specified in the Change Authorisation Note.

## Part E: Invoicing and Payment Terms

1. Supplier Invoices
   1. The Authority shall accept for processing any electronic invoice that complies with the Electronic Invoice Standard, provided that it is valid and undisputed.
   2. If the Supplier proposes to submit for payment an invoice that does not comply with the Electronic Invoice Standard the Supplier shall:
      1. comply with the requirements of the Authority’s e-invoicing system;
      2. prepare and provide to the Authority for approval of the format a template invoice within 10 Working Days of the Effective Date which shall include, as a minimum the details set out in Paragraph 1.3 together with such other information as the Authority may reasonably require to assess whether the Charges that will be detailed therein are properly payable; and
      3. make such amendments as may be reasonably required by the Authority if the template invoice outlined in 1.2.2 is not approved by the Authority.
   3. The Supplier shall ensure that each invoice is submitted in the correct format for the Authority’s e-invoicing system, or that it contains the following information:
      1. the date of the invoice;
      2. the name of the invoicing party;
      3. a unique invoice number;
      4. the Service Period or other period(s) to which the relevant Charge(s) relate;
      5. the correct reference for this Contract;
      6. the reference number of the purchase order to which it relates (if any);
      7. the dates between which the Services subject of each of the Charges detailed on the invoice were performed;
      8. a description of the Services and/or any other Deliverables;
      9. the pricing mechanism used to calculate the Charges (such as Guaranteed Maximum Price with Target Cost, Fixed Price, Time and Materials);
      10. any payments due in respect of Achievement of a Milestone, including the Milestone Achievement Certificate number for each relevant Milestone;
      11. the total Charges gross and net of any applicable deductions and, separately, the amount of any Reimbursable Expenses properly chargeable to the Authority under the terms of this Contract, and, separately, any VAT or other sales tax payable in respect of each of the same;
      12. details of any Service Credits or Delay Payments or similar deductions that shall apply to the Charges detailed on the invoice;
      13. reference to any reports required by the Authority in respect of the Services to which the Charges detailed on the invoice relate (or in the case of reports issued by the Supplier for validation by the Authority, then to any such reports as are validated by the Authority in respect of the Services);
      14. a contact name and telephone number of a responsible person in the Supplier’s finance department in the event of administrative queries;
      15. the banking details for payment to the Supplier via electronic transfer of funds (i.e. name and address of bank, sort code, account name and number); and
      16. where the Services have been structured into separate Service lines, the information at 1.3.1 to 1.3.15 of this Paragraph 1.3 shall be broken down in each invoice per Service line.
   4. The Supplier shall invoice the Authority in respect of Services in accordance with the requirements of Part B. The Supplier shall first submit to the Authority a draft invoice setting out the Charges payable. The Parties shall endeavour to agree the draft invoice within 5 Working Days of its receipt by the Authority, following which the Supplier shall be entitled to submit its invoice.
   5. Each invoice shall at all times be accompanied by Supporting Documentation. Any assessment by the Authority as to what constitutes Supporting Documentation shall not be conclusive and the Supplier undertakes to provide to the Authority any other documentation reasonably required by the Authority from time to time to substantiate an invoice.
   6. The Supplier shall submit all invoices and Supporting Documentation through the Authority’s electronic system [name] or if that is not possible to:
   7. [insert address or email address]
   8. with a copy (again including any Supporting Documentation) to such other person and at such place as the Authority may notify to the Supplier from time to time.
   9. All Supplier invoices shall be expressed in sterling or such other currency as shall be permitted by the Authority in writing.
   10. The Authority shall regard an invoice as valid only if it complies with the provisions of this Part E. Where any invoice does not conform to the Authority’s requirements set out in this Part E, or the Authority disputes the invoice, the Authority shall notify the Supplier without undue delay and the Supplier shall promptly issue a replacement invoice which shall comply with such requirements.
   11. If the Authority fails to consider and verify an invoice in accordance with Paragraphs 1.4 and 1.10, the invoice shall be regarded as valid and undisputed for the purpose of Paragraph 2.1 [Payment in 30 days] after a reasonable time has passed.
2. Payment Terms
   1. Subject to the relevant provisions of this Schedule, the Authority shall make payment to the Supplier within thirty (30) days of verifying that the invoice is valid and undisputed.
   2. Unless the Parties agree otherwise in writing, all Supplier invoices shall be paid in sterling by electronic transfer of funds to the bank account that the Supplier has specified on its invoice.

## Annex 1: Pricing Mechanism

1. Table 1: Supplier Personnel Rate Card for Calculation of Time and Materials Charges

| **Staff Grade** | **Day Rate (£)** |
| --- | --- |
|  |  |
|  |  |

1. Table 2: Maximum Time and Materials Charges

| **Charge Number** | **Maximum Time and Materials Charges (the cap) (£)** |
| --- | --- |
| [Service Line 1] | |
| [e.g. S1M1] |  |
| [e.g. S2M2] |  |
| [Service Line 2] | |
| [e.g. S2M1] |  |
| [e.g. S2M2] |  |
| [Service Line [X] - insert further rows as necessary] | |
| [etc.] |  |

1. Table 3: Day Cost for Calculation of Guaranteed Maximum Price with Target Cost Charges

| **Supplier Personnel Grade** | **Day Cost (£)** |
| --- | --- |
|  |  |
|  |  |

1. Table 4: Guaranteed Maximum Price with Target Costs Charges

| **Charge Number** | **Milestone Group (if applicable)** | **Target Cost (£)** | **Target Price (£)** | **Guaranteed Maximum Price (110% of Target Price) (£)** |
| --- | --- | --- | --- | --- |
| [Service Line 1] | | | | |
| [e.g. SL1M1] | [e.g. S1MG1] |  |  |  |
| [e.g. SL2M2] | [e.g. S1MG2] |  |  |  |
| [Service Line 2] | | | | |
| [e.g. SL2M3] | [e.g. S2MG1] |  |  |  |
| [e.g. SL2M4] | [e.g. S2MG2] |  |  |  |
| [Service Line [X] – insert further rows as necessary] | | | | |
| [etc.] | … |  |  |  |
|  |  |  |  |  |

1. Table 5: Fixed Prices

| **Charge** | **Fixed Charge (£)**  **[ ]** |
| --- | --- |
| [Service Line 1] | |
| [e.g. SL1M3] |  |
| [e.g. SL1SC1] |  |
| [e.g. SL1SC3] |  |
| [Service Line 2] | |
| [e.g. SL2M3] |  |
| [e.g. SL2SC1] |  |
| [e.g. SL2SC3] |  |
| [Service Line [X] – insert further rows as necessary] | |
| [etc.] |  |
|  |  |

1. Table 6: Firm Prices

| **Charge** | **Firm Charge (£)** |
| --- | --- |
| [Service Line 1] | |
| [e.g. SL1M4] |  |
| [e.g. SL1MS3] |  |
| [Service Line 2] | |
| [e.g. SL2M4] |  |
| [e.g. SL2MS3] |  |
| [Service Line [X] – insert further rows as necessary] | |
| [etc.] | … |

1. Table 7: Volume Charges

| **Charge Number** | **Unit** | **Number of units per Service Period** | **Charge per unit (£)** |
| --- | --- | --- | --- |
| [Service Line 1] | | | |
| [e.g. SL1VC1] |  | [ ] - [ ] | [ ] |
| [ ] - [ ] | [ ] |
| [ ] - [ ] | [ ] |
| [e.g. SL1VC2] |  | [ ] - [ ] | [ ] |
| [ ] - [ ] | [ ] |
| [ ] - [ ] | [ ] |
| [e.g. SL1VC3] |  | [ ] - [ ] | [ ] - [ ] |
|  | [ ] - [ ] | [ ] - [ ] |
|  | [ ] - [ ] | [ ] - [ ] |
| [Service Line 2] | | | |
| [e.g. SL2VC1] |  | [ ] - [ ] | [ ] |
| [ ] - [ ] | [ ] |
| [ ] - [ ] | [ ] |
| [e.g. SL2VC2] |  | [ ] - [ ] | [ ] |
| [ ] - [ ] | [ ] |
| [ ] - [ ] | [ ] |
| [e.g. SL2VC3] |  | [ ] - [ ] | [ ] - [ ] |
|  | [ ] - [ ] | [ ] - [ ] |
|  | [ ] - [ ] | [ ] - [ ] |
| [Service Line [X] – insert further rows as necessary] | | | |
| [etc.] | …. | [ ] - [ ] | [ ] |
|  | [ ] - [ ] | [ ] |
|  | [ ] - [ ] | [ ] |

## Annex 2: Charging Mechanism and Adjustments

1. Table 1: Milestone Payments and Delay Payments

| **Charge Number** | **Pricing Mechanism (FIX / FIRM / GMPTC / T&M)** | **CPP Milestone Charge Number** | **Delay Payments (if Key Milestone) (£ per day)** | | |
| --- | --- | --- | --- | --- | --- |
| **<3 months’ notice** | **3-6 months’ notice** | **>6 months’ notice** |
| [Service Line 1] | | | | | |
| [e.g. SL1M1] | [FIRM] | [e.g. S2M2] |  |  |  |
| [e.g. SL1M2] | [FIRM] | [e.g. S2M2] |  |  |  |
| [Service Line 2] | | | | | |
| [e.g. SL2M1] | [FIRM] | [e.g. S2M2] |  |  |  |
| [e.g. SL2M2] | [FIRM] | [e.g. S2M2] |  |  |  |
| [Service Line [X] – insert further rows as necessary] | | | | | |
| [etc.] |  |  |  |  |  |
|  |  |  |  |  |  |

1. Table 2: Service Charges

| **Charge Number** | **Pricing Mechanism (VOL / FIX / T&M)** | **Service Charge Trigger Event** | **Service Charge Expiration Trigger Event** |
| --- | --- | --- | --- |
| [Service Line 1] | | | |
| [e.g. SL1C1] | [VOL] | [e.g. Achievement of Milestone 4] |  |
| [e.g. SL1C2] | [FIX] |  |  |
| [Service Line 2] | | | |
| [e.g. SL2C1] | [VOL] | [e.g. Achievement of Milestone 4] |  |
| [e.g. SL2C2] | [FIX] |  |  |
| [Service Line [X] - insert further rows as necessary] | | | |
| [e.g. SLXC1] | [VOL] | [e.g. Achievement of Milestone 4] |  |
| [e.g. SLXC2] | [FIX] |  |  |

1. Table 3: Optional Services Milestone Payments

| **Charge Number** | **Pricing Mechanism (FIX / FIRM / GMPTC / T&M)** | **CPP Milestone Charge Number** | **Delay Payments (if Key Milestone) (£ per day)** |
| --- | --- | --- | --- |
| [e.g. OMS1] | [FIRM] | [e.g. OMS2] |  |
| [e.g. OMS2] | [FIRM] | [e.g. OMS2] |  |

1. Table 4: Optional Services Service Charges

| **Charge Number** | **Pricing Mechanism (VOL / FIX / T&M)** | **Service Charge Trigger Event** | **Service Charge Expiration Trigger Event** |
| --- | --- | --- | --- |
| [e.g. OSC1] | [VOL] | [e.g. Achievement of Milestone 6] |  |
| [e.g. OSC2] | [FIX] |  |  |

## Annex 3: Pro-forma Certificate of Costs

I [name of CFO or Director of Finance or equivalent as agreed in advance in writing with the Authority] of **[insert** name of Supplier], certify that the financial information provided as part of this Certificate of Costs, incurred in relation to the **[insert** name/reference for the Contract] (the “Contract”) in relation to the following [Milestone/Milestone Group]:

**[insert** details of Milestone/Milestone Group]

1. has been reasonably and properly incurred in accordance with [name of Supplier]’s books, accounts, other documents and records;
2. is accurate and not misleading in all key respects; and
3. is in conformity with the Contract and with all generally accepted accounting principles within the United Kingdom.

Signed [Director of Finance or equivalent]

[Name of Supplier]

## Annex 4: Risk Register

| Column 1 | Column 2 | Column 3 | Column 4 | Column 5 | Column 6 | Column 7 | Column 8 | Column 9 | Column 10 | Column 11 | Column 12 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Risk Number | Risk Name | Description of risk | Timing | Likelihood | Impact (£) | Impact (description) | Mitigation (description) | Cost of mitigation | Post-mitigation impact (£) | Forecast Contingency Costs | Owner |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |

## Annex 5: Allowable Assumptions

| Column 1 | Column 2 | Column 3 | Column 4 | Column 5 | Column 6 | Column 7 | Column 8 | Column 9 | Column 10 | Column 11 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ref | Description of proposed Allowable Assumption | Impact on the Implementation Plan if the Allowable Assumption is not accurate | Cost Impact (maximum, minimum and most likely values if the Allowable Assumption is not accurate) | Basis of Calculation of Cost Impact | Applicable Profit Margin | Charge Impact (maximum, minimum and most likely values if the Allowable Assumption is not accurate) | Verification Method (how the Supplier will verify the Allowable Assumption) | Trigger for Invocation (what will determine that the Implementation Plan and/or Financial Model may require adjustment for the Allowable Assumption) | Period of Impact (period that the updated assumption will have an impact) | Expiry Date (Date at which the Allowable Assumption expires) |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

Schedule 12

Payments on Termination

# Schedule 12: Payments on Termination

1. Definitions
   1. In this Schedule, the following definitions shall apply:

|  |  |
| --- | --- |
| “Applicable Supplier Personnel” | any Supplier Personnel who:   1. at the Termination Date:    1. are employees of the Supplier;    2. are Dedicated Supplier Personnel;    3. have not transferred (and are not in scope to transfer at a later date) to the Authority or the Replacement Supplier by virtue of the Employment Regulations; and 2. are dismissed or given notice of dismissal by the Supplier within:    1. 40 Working Days of the Termination Date; or    2. such longer period required by Law, their employment contract (as at the Termination Date) or an applicable collective agreement; and 3. have not resigned or given notice of resignation prior to the date of their dismissal by the Supplier; and 4. the Supplier can demonstrate to the satisfaction of the Authority:    1. are surplus to the Supplier’s requirements after the Termination Date notwithstanding its obligation to provide services to its other customers;    2. are genuinely being dismissed for reasons of redundancy; and    3. have been selected for redundancy by the Supplier on objective grounds other than the fact that the Supplier is entitled to reimbursement under this provision in respect of such employees; |
| “Breakage Costs Payment” | an amount equal to the Redundancy Costs and the Contract Breakage Costs as at the Termination Date as determined in accordance with Paragraph 3; |
| “Compensation Payment” | the payment calculated in accordance with Paragraph 9; |
| “Contract Breakage Costs” | the amounts payable by the Supplier to its Key Sub-contractors or other third parties (as applicable) for terminating all relevant Key Sub-contracts or Third Party Contracts as a direct result of the early termination of this Contract; |
| “Dedicated Supplier Personnel” | all Supplier Personnel then assigned to the Services or any part of the Services. If the Supplier is unsure as to whether Supplier Personnel are or should be regarded as so assigned, it shall consult with the Authority whose view shall be determinative provided that the employee has been materially involved in the provision of the Services or any part of the Services; |
| “Profit Already Paid” | the Supplier Profit paid or payable to the Supplier under this Contract for the period from the Effective Date up to (and including) the Termination Date; |
| “Redundancy Costs” | the total sum of any of the following sums paid to Applicable Supplier Personnel, each amount apportioned between the Supplier and the Authority based on the time spent by such employee on the Services as a proportion of the total Service duration:   1. any statutory redundancy payment; and 2. in respect of an employee who was a Transferring Former Supplier Employee or a Transferring Authority Employee, any contractual redundancy payment (or where such a contractual benefit on redundancy is a benefit payable from a pension scheme, the increase in cost to the Supplier as a net present value compared to the benefit payable on termination of employment without redundancy), provided that such employee was entitled to such contractual redundancy payment immediately prior to his or her transfer to the Supplier under the Employment Regulations; |
| “Request for Estimate” | a written request sent by the Authority to the Supplier, requiring that the Supplier provide it with an accurate estimate of the Termination Payment and Compensation Payment that would be payable if the Authority exercised its right under Clause 31.1.1 (*Termination by the Authority*) to terminate this Contract for convenience on a specified Termination Date; |
| “Shortfall Period” | has the meaning given in Paragraph 9.2; |
| “Termination Estimate” | has the meaning given in Paragraph 14.2; |
| “Total Costs Incurred” | the Costs incurred by the Supplier up to the Termination Date in the performance of this Contract and detailed in the Financial Model (but excluding Contract Breakage Costs, Redundancy Costs and any costs the Supplier would not otherwise be able to recover through the Charges) less any Deductions up to (and including) the Termination Date; |
| “Unrecovered Costs” | the Costs incurred by the Supplier in the performance of this Contract (as summarised in the Financial Model) to the extent that the same remain at the Termination Date to be recovered through Charges that but for the termination of this Contract would have been payable by the Authority after the Termination Date in accordance with Schedule 11 (*Charges and Invoicing*) as such Costs and Charges are forecast in the Financial Model; |
| “Unrecovered Payment” | an amount equal to the lower of:   1. the sum of the Unrecovered Costs and the Unrecovered Profit; and 2. the amount specified in Paragraph 7; and |
| “Unrecovered Profit” | (Total Costs Incurred x Anticipated Contract Life Profit Margin) - Profit Already Paid + Milestone Retentions remaining unpaid at the Termination Date. |

1. Termination Payment
   1. The Termination Payment payable pursuant to Clause 32.4 (*Payments by* *the Authority*) shall be an amount equal to the aggregate of the Breakage Costs Payment and the Unrecovered Payment.
2. Breakage Costs Payment
   1. The Supplier may recover through the Breakage Costs Payment only those costs incurred by the Supplier directly as a result of the termination of this Contract which:
      1. would not have been incurred had this Contract continued until expiry of the Initial Term, or in the event that the Term has been extended, the expiry of the Extension Period;
      2. are unavoidable, proven, reasonable, and not capable of recovery;
      3. are incurred under arrangements or agreements that are directly associated with this Contract;
      4. are not Contract Breakage Costs relating to contracts or Sub-contracts with Affiliates of the Supplier; and
      5. relate directly to the termination of the Services.
3. Limitation on Breakage Costs Payment
   1. The Breakage Costs Payment shall not exceed the lower of:
      1. the relevant limit set out in Annex 1; and
      2. 120% of the estimate for the Breakage Costs Payment set out in any relevant Termination Estimate.
4. Redundancy Costs
   1. The Authority shall not be liable under this Schedule for any costs associated with Supplier Personnel (whether relating to redundancy, redeployment or otherwise) other than the Redundancy Costs.
   2. Where the Supplier can demonstrate that a member of Supplier Personnel will be made redundant following termination of this Contract, but redeployment of such person is possible and would offer value for money to the Authority when compared with redundancy, then the Authority shall pay the Supplier the actual direct costs incurred by the Supplier or its Sub-contractor arising out of the redeployment of such person (including retraining and relocation costs) subject to a maximum amount of £30,000 per relevant member of the Supplier Personnel.
5. Contract Breakage Costs
   1. The Supplier shall be entitled to Contract Breakage Costs only in respect of Third Party Contracts or Sub-contracts which:
      1. are not assigned or novated to a Replacement Supplier at the request of the Authority in accordance with Schedule 21 (*Exit Management*); and
      2. the Supplier can demonstrate:
         1. are surplus to the Supplier’s requirements after the Termination Date, whether in relation to use internally within its business or in providing services to any of its other customers; and
         2. have been entered into by it in the ordinary course of business.
   2. The Supplier shall seek to negotiate termination of any Third Party Contracts or Sub-contracts with the relevant third party or Sub-contractor (as the case may be) using all reasonable endeavours to minimise the cancellation or termination charges.
   3. Except with the prior written agreement of the Authority, the Authority shall not be liable for any costs (including cancellation or termination charges) that the Supplier is obliged to pay in respect of:
      1. the termination of any contractual arrangements for occupation of, support of and/or services provided for Supplier premises which may arise as a consequence of the termination of this Contract; and/or
      2. Assets not yet installed at the Termination Date.
6. Unrecovered Payment
   1. The Unrecovered Payment shall not exceed the lowest of:
      1. the relevant limit set out in Annex 1;
      2. 120% of the estimate for the Unrecovered Payment set out in any relevant Termination Estimate; and
      3. the Charges that but for the termination of this Contract would have been payable by the Authority after the Termination Date in accordance with Schedule 11 (*Charges and Invoicing*) as forecast in the Financial Model.
7. Mitigation of Contract Breakage Costs, Redundancy Costs and Unrecovered Costs
   1. The Supplier agrees to use all reasonable endeavours to minimise and mitigate Contract Breakage Costs, Redundancy Costs and Unrecovered Costs by:
      1. the appropriation of Assets, employees and resources for other purposes;
      2. at the Authority’s request, assigning any Third Party Contracts and Sub-contracts to the Authority or a third party acting on behalf of the Authority; and
      3. in relation Third Party Contracts and Sub-contract that are not to be assigned to the Authority or to another third party, terminating those contracts at the earliest possible date without breach or where contractually permitted.
   2. If Assets, employees and resources can be used by the Supplier for other purposes, then there shall be an equitable reduction in the Contract Breakage Costs, Redundancy Costs and Unrecovered Costs payable by the Authority or a third party to the Supplier. In the event of any Dispute arising over whether the Supplier can use any Assets, employees and/or resources for other purposes and/or over the amount of the relevant equitable reduction, the Dispute shall be referred to an Expert for determination in accordance with the procedure detailed in Schedule 19 (*Dispute Resolution Procedure*).
8. Compensation Payment
   1. The Compensation Payment payable pursuant to Clause 32.4 (*Payments* *by the Authority*) shall be an amount equal to the total forecast Charges over the Shortfall Period (as stated in the Financial Model) multiplied by the Anticipated Contract Life Profit Margin.
   2. For the purposes of Paragraph 9.1, the “Shortfall Period” means:
      1. where the Authority terminates this Contract pursuant to Clause 31.1.1 (*Termination by the Authority*), a number of days equal to the number of days by which the notice given (or deemed given pursuant to Paragraph 2.1.1 of Part D of Schedule 11 (*Charges and Invoicing*)) falls short of three hundred and sixty-five (365) days; or
      2. where the Supplier terminates this Contract pursuant to Clause 31.3.1 (*Termination by the Supplier*), a number of days equal to the number of days by which the period from (and including) the date of the non-payment by the Authority to (and including) the Termination Date falls short of 365 days,

but in each case subject to the limit set out in Paragraph 9.3.

* 1. The Compensation Payment shall be no greater than the lower of:
     1. the relevant limit set out in Annex 1; and
     2. 120% of the estimate for the Compensation Payment set out in the relevant Termination Estimate.

1. Full and Final Settlement
   1. Any Termination Payment and/or Compensation Payment paid under this Schedule shall be in full and final settlement of any claim, demand and/or proceedings of the Supplier in relation to any termination by the Authority pursuant to Clause 31.1.1 (*Termination by the Authority*) or termination by the Supplier pursuant to Clause 31.3.1 (*Termination by the Supplier*) (as applicable), and the Supplier shall be excluded from all other rights and remedies it would otherwise have been entitled to in respect of any such termination.
2. Invoicing for the Payments on Termination
   1. All sums due under this Schedule shall be payable by the Authority to the Supplier in accordance with the payment terms set out in Schedule 11 (*Charges and Invoicing*).
3. Set Off
   1. The Authority shall be entitled to set off any outstanding liabilities of the Supplier against any amounts that are payable by it pursuant to this Schedule.
4. No Double Recovery
   1. If any amount payable under this Schedule (in whole or in part) relates to or arises from any Transferring Assets then, to the extent that the Authority makes any payments pursuant to Schedule 21 (*Exit Management*) in respect of such Transferring Assets, such payments shall be deducted from the amount payable pursuant to this Schedule.
   2. The value of the Termination Payment and/or the Compensation Payment shall be reduced or extinguished to the extent that the Supplier has already received the Charges or the financial benefit of any other rights or remedy given under this Contract so that there is no double counting in calculating the relevant payment.
   3. Any payments that are due in respect of the Transferring Assets shall be calculated in accordance with the provisions of the Exit Plan.
5. Estimate of Termination Payment and Compensation Payment
   1. The Authority may issue a Request for Estimate at any time during the Term provided that no more than 2 Requests for Estimate may be issued in any 6 month period.
   2. The Supplier shall within 20 Working Days of receiving the Request for Estimate (or such other timescale agreed between the Parties), provide an accurate written estimate of the Termination Payment and the Compensation Payment that would be payable by the Authority based on a postulated Termination Date specified in the Request for Estimate (such estimate being the “Termination Estimate”). The Termination Estimate shall:
      1. be based on the relevant amounts set out in the Financial Model;
      2. include:
         1. details of the mechanism by which the Termination Payment is calculated;
         2. full particulars of the estimated Contract Breakage Costs in respect of each Sub-contract or Third Party Contract and appropriate supporting documentation; and
         3. such information as the Authority may reasonably require; and
      3. state the period for which that Termination Estimate remains valid, which shall be not less than 20 Working Days.
   3. The Supplier acknowledges that issue of a Request for Estimate shall not be construed in any way as to represent an intention by the Authority to terminate this Contract.
   4. If the Authority issues a Termination Notice to the Supplier within the stated period for which a Termination Estimate remains valid, the Supplier shall use the same mechanism to calculate the Termination Payment as was detailed in the Termination Estimate unless otherwise agreed in writing between the Supplier and the Authority.

## Annex 1: Maximum Payments on Termination

The table below sets out, by Contract Year, the maximum amount of the Unrecovered Payment, Breakage Costs Payment and Compensation Payment that the Authority shall be liable to pay to the Supplier pursuant to this Contract:

| Termination Date | Maximum Unrecovered Payment | Maximum Breakage Costs Payment | Maximum Compensation Payment |
| --- | --- | --- | --- |
| Anytime in the first Contract Year |  |  |  |
| Anytime in the second Contract Year |  |  |  |
| Anytime in Contract Years 3 – [x] |  |  |  |

Schedule 13

Benchmarking

# Schedule 13: Benchmarking

1. Definitions
   1. In this Schedule, the following definitions shall apply:

|  |  |
| --- | --- |
| “Benchmarked Service” | a Service that the Authority elects to include in a Benchmark Review under Paragraph 2.3; |
| “Benchmarker” | the independent third party appointed under Paragraph 3.1; |
| “Benchmark Report” | the report produced by the Benchmarker following the Benchmark Review as further described in Paragraph 5; |
| “Benchmark Review” | a review of one or more of the Services carried out in accordance with Paragraph 4 to determine whether those Services represent Good Value; |
| “Comparable Service” | in relation to a Benchmarked Service, a service that is identical or materially similar to the Benchmarked Service (including in terms of scope, specification, volume and quality of performance); |
| “Comparison Group” | in relation to a Comparable Service, a sample group of organisations providing the Comparable Service identified by the Benchmarker under Paragraph 4.8 which consists of organisations which are either of similar size to the Supplier or which are similarly structured in terms of their business and their service offering so as to be (in the Benchmarker’s professional opinion) fair comparators with the Supplier or which, in the professional opinion of the Benchmarker, are best practice organisations and, where there are a reasonable number of such organisations, referencing only those organisations that are carrying on at least a significant part of their business within the United Kingdom; |
| “Equivalent Services Data” | in relation to a Comparable Service, data derived from an analysis of the Comparable Service provided by the Comparison Group as adjusted in accordance with Paragraphs 4.8.1 and 4.9 provided that the Benchmarker shall not use any such data that relates to a period which ended more than 36 months prior to the date of the appointment of the Benchmarker; |
| “Good Value” | in relation to a Benchmarked Service, that:   1. having taken into account the Performance Indicators and Target Performance Levels, the value for money of the Charges attributable to that Benchmarked Service is at least as good as the value for money of the Upper Quartile; and 2. any Performance Indicators and Target Performance Levels applicable to that Benchmarked Service are, having taken into account the Charges, equal to or better than the median service levels for the Comparable Service using Equivalent Services Data; and |
| “Upper Quartile” | the top 25% of instances of provision of a Comparable Service by members of the Comparison Group ranked by best value for money to the recipients of that Comparable Service. |

1. Frequency, Purpose and Scope of Benchmark Review
   1. The Authority may, by written notice to the Supplier, require a Benchmark Review of any or all of the Services in order to establish whether a Benchmarked Service is, and/or the Benchmarked Services as a whole are, Good Value.
   2. The Authority shall not be entitled to carry out a Benchmark Review of any Services during the 12 month period from the Operational Service Commencement Date for those Services, nor at intervals of less than 12 months after any previous Benchmark Review relating to the same Services.
   3. The Services that are to be the Benchmarked Services shall be identified by the Authority in the notice given under Paragraph 2.1.
2. Appointment of Benchmarker
   1. The Authority shall appoint as the Benchmarker to carry out the Benchmark Review either an organisation on the list of organisations set out in Annex 1 or such other organisation as may be agreed in writing between the Parties.
   2. The Authority shall, at the written request of the Supplier, require the Benchmarker to enter into a confidentiality agreement with the Supplier in, or substantially in, the form set out in Annex 2.
   3. The costs and expenses of the Benchmarker and the Benchmark Review shall be shared equally between both Parties provided that each Party shall bear its own internal costs of the Benchmark Review. The Benchmarker shall not be compensated on a contingency fee or incentive basis.
   4. The Authority shall be entitled to pay the Benchmarker’s costs and expenses in full and to recover the Supplier’s share from the Supplier.
3. Benchmark Review
   1. The Authority shall require the Benchmarker to produce, and to send to each Party for approval, a draft plan for the Benchmark Review within 10 Working Days after the date of the appointment of the Benchmarker, or such longer period as the Benchmarker shall reasonably request in all the circumstances. The plan must include:
      1. a proposed timetable for the Benchmark Review;
      2. a description of the information that the Benchmarker requires each Party to provide;
      3. a description of the benchmarking methodology to be used;
      4. a description that clearly illustrates that the benchmarking methodology to be used is capable of fulfilling the benchmarking objectives under Paragraph 2.1;
      5. an estimate of the resources required from each Party to underpin the delivery of the plan;
      6. a description of how the Benchmarker will scope and identify the Comparison Group;
      7. details of any entities which the Benchmarker proposes to include within the Comparison Group; and
      8. if in the Benchmarker’s professional opinion there are no Comparable Services or the number of entities carrying out Comparable Services is insufficient to create a Comparison Group, a detailed approach for meeting the relevant benchmarking objective(s) under Paragraph 2.1 using a proxy for the Comparison Services and/or Comparison Group as applicable.
   2. The Parties acknowledge that the selection and or use of proxies for the Comparison Group (both in terms of number and identity of entities) and Comparable Services shall be a matter for the Benchmarker’s professional judgment.
   3. Each Party shall give notice in writing to the Benchmarker and to the other Party within 10 Working Days after receiving the draft plan either approving the draft plan or suggesting amendments to that plan which must be reasonable Where a Party suggests amendments to the draft plan pursuant to this Paragraph 4.3, the Benchmarker shall, if it believes the amendments are reasonable, produce an amended draft plan. Paragraph 4.1 and this Paragraph 4.3 shall apply to any amended draft plan.
   4. Failure by a Party to give notice under Paragraph 4.3 shall be treated as approval of the draft plan by that Party. If the Parties fail to approve the draft plan within 30 Working Days of its first being sent to them pursuant to Paragraph 4.1 then the Benchmarker shall prescribe the plan.
   5. Once the plan is approved by both Parties or prescribed by the Benchmarker, the Benchmarker shall carry out the Benchmark Review in accordance with the plan. Each Party shall procure that all the information described in the plan, together with any additional information reasonably required by the Benchmarker is provided to the Benchmarker without undue delay. If the Supplier fails to provide any information requested from it by the Benchmarker and described in the plan, such failure shall constitute a material Default for the purposes of Clause 25.1.3 (*Rectification Plan Process*).
   6. Each Party shall co-operate fully with the Benchmarker, including by providing access to records, technical documentation, premises, equipment, systems and personnel at times reasonably requested by the Benchmarker, provided that the Benchmarker shall be instructed to minimise any disruption to the Services.
   7. Either Party may provide additional material to the Benchmarker to assist the Benchmarker in conducting the Benchmark Review.
   8. Once it has received the information it requires, the Benchmarker shall:
      1. finalise the sample of entities constituting the Comparison Group and collect data relating to Comparable Services. The final selection of the Comparison Group (both in terms of number and identity of entities) and of the Comparable Services shall be a matter for the Benchmarker’s professional judgment;
      2. derive the Equivalent Services Data by applying the adjustment factors listed in Paragraph 4.9 and from an analysis of the Comparable Services;
      3. derive the relative value for money of the charges payable for the Comparable Services using the Equivalent Services Data and from that derive the Upper Quartile;
      4. derive the median service levels relating to the Comparable Services using the Equivalent Services Data;
      5. compare the value for money of the Charges attributable to the Benchmarked Services (having regard in particular to the applicable Performance Indicators and Target Performance Levels) to the value for money of the Upper Quartile;
      6. compare the Performance Indicators and Target Performance Levels attributable to the Benchmarked Services (having regard to the Charges and Service Credits) with the median service levels using the Equivalent Services Data; and
      7. determine whether or not each Benchmarked Service is and/or the Benchmarked Services as a whole are, Good Value.
   9. The Benchmarker shall have regard to the following matters when performing a comparative assessment of a Benchmarked Service and a Comparable Service in order to derive Equivalent Services Data:
      1. the contractual and business environment under which the Services are being provided (including the scope, scale, complexity and geographical spread of the Services);
      2. any front-end investment and development costs of the Supplier;
      3. the Supplier’s risk profile including the financial, performance or liability risks associated with the provision of the Services as a whole;
      4. the extent of the Supplier’s management and contract governance responsibilities;
      5. any other reasonable factors demonstrated by the Supplier, which, if not taken into consideration, could unfairly cause the Supplier’s pricing to appear non-competitive (such as erroneous costing, non-sustainable behaviour including excessive consumption of energy or over-aggressive pricing).
4. Benchmark Report
   1. The Benchmarker shall be required to prepare a Benchmark Report and deliver it simultaneously to both Parties, at the time specified in the plan approved under Paragraph 4, setting out its findings. The Benchmark Report shall:
      1. include a finding as to whether or not each Benchmarked Service is and/or whether the Benchmarked Services as a whole are, Good Value;
      2. include other findings (if any) regarding the quality and competitiveness or otherwise of those Services;
      3. if any Benchmarked Service is not Good Value, or the Benchmarked Services as a whole are not Good Value, specify the changes that would be required to the Charges, Performance Indicators and/or Target Performance Levels, that would be required to make that Benchmarked Service or those Benchmarked Services as a whole Good Value; and
      4. illustrate the method used for any normalisation of the Equivalent Services Data
   2. The Benchmarker shall act as an expert and not as an arbitrator.
   3. If the Benchmark Report states that any Benchmarked Service is not Good Value or that the Benchmarked Services as a whole are not Good Value, then the Supplier shall (subject to Paragraphs 5.5 and 5.6) implement the changes set out in the Benchmark Report as soon as reasonably practicable within timescales agreed with the Authority but in any event within no more than 3 months. Any associated changes to the Charges shall take effect only from the same date and shall not be retrospective.
   4. The Supplier acknowledges and agrees that Benchmark Reviews shall not result in any increase to the Charges, disapplication of the Performance Indicators or any reduction in the Target Performance Levels.
   5. The Supplier shall be entitled to reject any Benchmark Report if the Supplier reasonably considers that the Benchmarker has not followed the procedure for the related Benchmark Review as set out in this Schedule in any material respect.
   6. The Supplier shall not be obliged to implement any Benchmark Report to the extent this would cause the Supplier to provide the Services at a loss (as determined, by reference to the Financial Model), or to the extent the Supplier cannot technically implement the recommended changes.
   7. In the event of any Dispute arising over whether the Benchmarker has followed the procedure for the related Benchmark Review under Paragraph 5.5 and/or any matter referred to in Paragraph 5.6, the Dispute shall be referred to Expert Determination. For the avoidance of doubt in the event of a Dispute between the Parties, the Authority shall continue to pay the Charges to the Supplier in accordance with the terms of this Contract and the Performance Indicators and Target Performance Levels shall remain unchanged pending the conclusion of the Expert Determination.
   8. On conclusion of the Expert Determination:
      1. if the Expert determines that all or any part of the Benchmark Report recommendations regarding any reduction in the Charges shall be implemented by the Supplier, the Supplier shall immediately repay to the Authority the difference between the Charges paid by the Authority up to and including the date of the Expert’s determination and the date upon which the recommended reduction in Charges should have originally taken effect pursuant to Paragraph 5.3 together with interest thereon at the applicable rate under the Late Payment Of Commercial Debts (Interest) Act 1998; and
      2. if the Expert determines that all or any part of the Benchmark Report recommendations regarding any changes to the Performance Indicators and/or Target Performance Levels shall be implemented by the Supplier:
         1. the Supplier shall immediately implement the relevant changes;
         2. the Supplier shall immediately pay an amount equal to any Service Credits which would have accrued up to and including the date of the Expert’s determination if the relevant changes had taken effect on the date determined pursuant to Paragraph 5.3 together with interest thereon at the applicable rate under the Late Payment Of Commercial Debts (Interest) Act 1998; and
         3. the relevant changes shall thereafter be subject to the Change Control Procedure for the purposes of formalising and documenting the relevant change or amendment for the purposes of this Contract.
   9. Any failure by the Supplier to implement the changes as set out in the Benchmark Report in accordance with the relevant timescales determined in accordance with Paragraph 5.3 (unless the provisions of Paragraph 5.6 and/or Paragraph 5.7 apply) or in accordance with Paragraph 5.8 shall, without prejudice to any other rights or remedies of the Authority, constitute a Supplier Termination Event.

## Annex 1: Approved Benchmarkers

## Annex 2: Confidentiality Agreement

CONFIDENTIALITY AGREEMENT

THIS AGREEMENT is made on [date]

BETWEEN:

1. [insert name] of **[insert** address] (the “Supplier”); and
2. [insert name] of **[insert** address] (the “Benchmarker” and together with the Supplier, the “Parties”).

WHEREAS:

(A) **[insert** name of Authority] (the “Authority”) and the Supplier are party to a contract dated **[insert** date] (the “Contract”) for the provision by the Supplier of **[insert** brief description of services] to the Authority.

(B) The Benchmarker is to receive Confidential Information from the Supplier for the purpose of carrying out a benchmarking review for the Authority of one or more of such services pursuant to the terms of the Contract (the “Permitted Purpose”).

IT IS AGREED as follows:

1. Interpretation
   1. In this Agreement, unless the context otherwise requires:

|  |  |
| --- | --- |
| “Confidential Information” | means:   1. Information, including all personal data within the meaning of the Data Protection Act 2018, and however it is conveyed, provided by the Supplier to the Benchmarker pursuant to this Agreement that relates to:    1. the Supplier; or    2. the operations, business, affairs, developments, intellectual property rights, trade secrets, know-how and/or personnel of the Supplier; 2. other Information provided by the Supplier pursuant to this Agreement to the Benchmarker that is clearly designated as being confidential or equivalent or that ought reasonably to be considered to be confidential which comes (or has come) to the Benchmarker’s attention or into the Benchmarker’s possession in connection with the Permitted Purpose; 3. discussions, negotiations, and correspondence between the Supplier or any of its directors, officers, employees, consultants or professional advisers and the Benchmarker or any of its directors, officers, employees, consultants and professional advisers in connection with the Permitted Purpose and all matters arising therefrom; and 4. Information derived from any of the above,   but not including any Information that:   1. was in the possession of the Benchmarker without obligation of confidentiality prior to its disclosure by the Supplier; 2. the Benchmarker obtained on a non-confidential basis from a third party who is not, to the Benchmarker’s knowledge or belief, bound by a confidentiality agreement with the Supplier or otherwise prohibited from disclosing the information to the Benchmarker; 3. was already generally available and in the public domain at the time of disclosure otherwise than by a breach of this Agreement or breach of a duty of confidentiality; or 4. was independently developed without access to the Confidential Information; |
| “Information” | means all information of whatever nature, however conveyed and in whatever form, including in writing, orally, by demonstration, electronically and in a tangible, visual or machine-readable medium (including CD-ROM, magnetic and digital form); and |
| “Permitted Purpose” | has the meaning given to that expression in recital (B) to this Agreement. |

* 1. In this Agreement:
     1. a reference to any gender includes a reference to other genders;
     2. the singular includes the plural and vice versa;
     3. the words “include” and cognate expressions shall be construed as if they were immediately followed by the words “without limitation”;
     4. references to any statutory provision include a reference to that provision as modified, replaced, amended and/or re-enacted from time to time (before or after the date of this Agreement) and any prior or subsequent subordinate legislation made under it;
     5. headings are included for ease of reference only and shall not affect the interpretation or construction of this Agreement; and
     6. references to Clauses are to clauses of this Agreement.

1. Confidentiality Obligations
   1. In consideration of the Supplier providing Confidential Information to the Benchmarker, the Benchmarker shall:
      1. treat all Confidential Information as secret and confidential;
      2. have in place and maintain proper security measures and procedures to protect the confidentiality of the Confidential Information (having regard to its form and nature);
      3. not disclose or permit the disclosure of any of the Confidential Information to any other person without obtaining the prior written consent of the Supplier or, if relevant, other owner or except as expressly set out in this Agreement;
      4. not transfer any of the Confidential Information outside the United Kingdom;
      5. not use or exploit any of the Confidential Information for any purpose whatsoever other than the Permitted Purpose;
      6. immediately notify the Supplier in writing if it suspects or becomes aware of any unauthorised access, copying, use or disclosure in any form of any of the Confidential Information; and
      7. once the Permitted Purpose has been fulfilled:
         1. destroy or return to the Supplier all documents and other tangible materials that contain any of the Confidential Information;
         2. ensure, so far as reasonably practicable, that all Confidential Information held in electronic, digital or other machine-readable form ceases to be readily accessible (other than by the information technology staff of the Benchmarker) from any computer, word processor, voicemail system or any other device; and
         3. make no further use of any Confidential Information.
2. Permitted Disclosures
   1. The Benchmarker may disclose Confidential Information to those of its directors, officers, employees, consultants and professional advisers who:
      1. reasonably need to receive the Confidential Information in connection with the Permitted Purpose; and
      2. have been informed by the Benchmarker of the confidential nature of the Confidential Information; and
      3. have agreed to terms similar to those in this Agreement.
   2. The Benchmarker shall be entitled to disclose Confidential Information to the Authority for the Permitted Purpose and to any Expert appointed in relation to a Dispute as referred to in Paragraph 5.7 of this Schedule 13 (*Benchmarking*) to the Contract.
   3. The Benchmarker shall be entitled to disclose Confidential Information to the extent that it is required to do so by applicable law or by order of a court or other public body that has jurisdiction over the Benchmarker.
   4. Before making a disclosure pursuant to Clause 3.3, the Benchmarker shall, if the circumstances permit:
      1. notify the Supplier in writing of the proposed disclosure as soon as possible (and if possible before the court or other public body orders the disclosure of the Confidential Information); and
      2. ask the court or other public body to treat the Confidential Information as confidential.
3. General
   1. The Benchmarker acknowledges and agrees that all property, including intellectual property rights, in Confidential Information disclosed to it by the Supplier shall remain with and be vested in the Supplier.
   2. This Agreement does not include, expressly or by implication, any representations, warranties or other obligations:
      1. to grant the Benchmarker any licence or rights other than as may be expressly stated in this Agreement;
      2. to require the Supplier to disclose, continue disclosing or update any Confidential Information; or
      3. as to the accuracy, efficacy, completeness, capabilities, safety or any other qualities whatsoever of any Information or materials provided pursuant to or in anticipation of this Agreement.
   3. The rights, powers and remedies provided in this Agreement are cumulative and not exclusive of any rights, powers or remedies provided by law. No failure or delay by either Party to exercise any right, power or remedy will operate as a waiver of it nor will any partial exercise preclude any further exercise of the same, or of some other right, power or remedy.
   4. Without prejudice to any other rights or remedies that the Supplier may have, the Benchmarker acknowledges and agrees that damages alone may not be an adequate remedy for any breach by the Benchmarker of any of the provisions of this Agreement. Accordingly, the Benchmarker acknowledges that the Supplier shall be entitled to the remedies of injunction and specific performance as well as any other equitable relief for any threatened or actual breach of this Agreement and/or breach of confidence and that no proof of special damages shall be necessary for the enforcement of such remedies.
   5. The maximum liability of the Benchmarker to the Supplier for any breach of this Agreement shall be limited to ten million pounds (£10,000,000).
   6. For the purposes of the Contracts (Rights of Third Parties) Act 1999 no one other than the Parties has the right to enforce the terms of this Agreement.
   7. Each Party shall be responsible for all costs incurred by it or on its behalf in connection with this Agreement.
   8. This Agreement may be executed in any number of counterparts and by the Parties on separate counterparts, but shall not be effective until each Party has executed at least one counterpart. Each counterpart shall constitute an original of this Agreement, but all the counterparts shall together constitute but one and the same instrument.
4. Notices
   1. Any notice to be given under this Agreement (each a “Notice”) shall be given in writing and shall be delivered by hand and shall be deemed to have been duly given at the time of delivery provided that such Notice is sent to the relevant physical address, and expressly marked for the attention of the relevant individual, set out in Clause 5.2.
   2. Any Notice:
      1. if to be given to the Supplier shall be sent to:

[Address]

Attention: [Contact name and/or position, e.g. “The Finance Director”]

* + 1. if to be given to the Benchmarker shall be sent to:

[Name of Organisation]

[Address]

Attention: [ ]

1. Governing law
   1. This Agreement shall be governed by, and construed in accordance with, English law and any matter claim or dispute arising out of or in connection with this Agreement whether contractual or non-contractual, shall be governed by and determined in accordance with English law.
   2. Each Party hereby irrevocably submits to the exclusive jurisdiction of the English courts in respect of any claim or dispute arising out of or in connection with this Agreement.

IN WITNESS of the above this Agreement has been signed by the duly authorised representatives of the Parties on the date which appears at the head of page 1.

For and on behalf of [name of Supplier]

|  |  |
| --- | --- |
| Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Date: |
| Name: | Position: |

For and on behalf of [name of Benchmarker]

|  |  |
| --- | --- |
| Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Date: |
| Name: | Position: |

Schedule 14

Financial Distress

# Schedule 14: Financial Distress

*[Guidance: This template Schedule provides the Authority with the option of using Credit Ratings and/or Financial Indicators for the purposes of the Financial Distress Provisions. Authorities may use any combination of these indicators to suit their own requirements and may delete or amend as required. Authorities should ensure that the drafting of any Financial Indicators aligns with the financial standing criteria used during the Conditions of Participation of the procurement.]*

1. Definitions
   1. In this Schedule, the following definitions shall apply:

|  |  |
| --- | --- |
| “Applicable Financial Indicators” | the financial indicators from Paragraph 5.1 of this Schedule which are to apply to the Monitored Suppliers as set out in Paragraph 5.2 of this Schedule; |
| "Authorised Financial Representative" | a statutory director of the Supplier or a sufficiently senior member of the Supplier's management team who has the authority to act on behalf of the Supplier in relation to financial matters; |
| “Board” | the Supplier’s board of directors; |
| “Board Confirmation” | written confirmation from the Board in accordance with Paragraph 8 of this Schedule; |
| “Credit Rating Level” | a credit rating level as specified in Annex 1 of this Schedule; |
| “Credit Rating Threshold” | the minimum Credit Rating Level for each entity in the FDE Group as set out in Annex 2 of this Schedule; |
| “FDE Group” | the [Supplier, Key Sub-contractors, [the Guarantor] and the [Monitored Suppliers]]; |
| “Financial Indicators” | in respect of the Supplier, Key Sub-contractors and the Guarantor, means each of the financial indicators set out at Paragraph 5.1 of this Schedule; and in respect of each Monitored Supplier, means those Applicable Financial Indicators; |
| “Financial Target Thresholds” | the target thresholds for each of the Financial Indicators set out at Paragraph 5.1 of this Schedule; |
| “Monitored Suppliers” | those entities specified at Paragraph 5.2 of this Schedule; and |
| “Rating Agencies” | the rating agencies listed in Annex 1 of this Schedule. |

1. Warranties and Duty to Notify
   1. The Supplier warrants and represents to the Authority for the benefit of the Authority that as at the Effective Date:
      1. the long term credit ratings issued for each entity in the FDE Group by each of the Rating Agencies are as set out in Annex 2 of this Schedule; and
      2. the financial position or, as appropriate, the financial performance of each of the Supplier, Guarantor and Key Sub-contractors satisfies the Financial Target Thresholds.
   2. The Supplier shall promptly notify (or shall procure that its auditors promptly notify) the Authority in writing if there is any downgrade in the credit rating issued by any Rating Agency for any entity in the FDE Group (and in any event within 5 Working Days of the occurrence of the downgrade).
   3. The Supplier shall:
      1. regularly monitor the credit ratings of each entity in the FDE Group with the Rating Agencies;
      2. monitor and report on the Financial Indicators for each entity in the FDE Group against the Financial Target Thresholds at least at the frequency set out for each at Paragraph 5.1 (where specified) and in any event, on a regular basis and no less than once a year within one hundred and twenty (120) days after the Accounting Reference Date; and
      3. promptly notify (or shall procure that its auditors promptly notify) the Authority in writing following the occurrence of a Financial Distress Event or any fact, circumstance or matter which could cause a Financial Distress Event (and in any event, ensure that such notification is made within 10 Working Days of the date on which the Supplier first becomes aware of the Financial Distress Event or the fact, circumstance or matter which could cause a Financial Distress Event).
   4. For the purposes of determining whether a Financial Distress Event has occurred pursuant to the provisions of Paragraph 3.1.1, and for the purposes of determining relief under Paragraph 7.1, the credit rating of an FDE Group entity shall be deemed to have dropped below the applicable Credit Rating Threshold if:
      1. any of the Rating Agencies have given a Credit Rating Level for that entity which is below the applicable Credit Rating Threshold; or
      2. a Rating Agency that is specified as holding a Credit Rating for an entity as set out at Annex 2 of this Schedule ceases to hold a Credit Rating for that entity.
   5. Each report submitted by the Supplier pursuant to Paragraph 2.3.2 shall:
      1. be a single report with separate sections for each of the FDE Group entities;
      2. contain a sufficient level of information to enable the Authority to verify the calculations that have been made in respect of the Financial Indicators;
      3. include key financial and other supporting information (including any accounts data that has been relied on) as separate annexes;
      4. be based on the audited accounts for the date or period on which the Financial Indicator is based or, where the Financial Indicator is not linked to an accounting period or an accounting reference date, on unaudited management accounts prepared in accordance with their normal timetable; and
      5. include a history of the Financial Indicators reported by the Supplier in graph form to enable the Authority to easily analyse and assess the trends in financial performance.
2. Financial Distress Events
   1. The following shall be Financial Distress Events:
      1. the credit rating of an FDE Group entity dropping below the applicable Credit Rating Threshold;
      2. an FDE Group entity issuing a profits warning to a stock exchange or making any other public announcement, in each case about a material deterioration in its financial position or prospects;
      3. there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of an FDE Group entity;
      4. an FDE Group entity committing a material breach of covenant to its lenders;
      5. a Key Sub-contractor notifying the Authority that the Supplier has not satisfied any material sums properly due under a specified invoice and not subject to a genuine dispute;
      6. any FDE Group entity extends the filing period for filing its accounts with the Registrar of Companies so that the filing period ends more than 9 months after its accounting reference date without an explanation to the Authority which the Authority (acting reasonably) considers to be adequate;
      7. any FDE Group entity is late to file its annual accounts without a public notification or an explanation to the Authority which the Authority, acting reasonably, considers to be adequate;
      8. the directors and/or external auditors of any FDE Group entity conclude that a material uncertainty exists in relation to that FDE Group entity’s going concern in the annual report including in a reasonable but plausible downside scenario. This includes, but is not limited to, commentary about liquidity and trading prospects in the reports from directors or external auditors;
      9. any of the following:
         1. any FDE Group entity makes a public announcement which contains adverse commentary with regards to that FDE Group entity’s liquidity and trading and trading prospects, such as but not limited to, a profit warning or ability to trade as a going concern;
         2. commencement of any litigation against an FDE Group entity with respect to financial indebtedness greater than £5m or obligations under a service contract with a total contract value greater than £5m;
         3. non-payment by an FDE Group entity of any financial indebtedness;
         4. any financial indebtedness of an FDE Group entity becoming due as a result of an event of default;
         5. the cancellation or suspension of any financial indebtedness in respect of an FDE Group entity; or
         6. the external auditor of an FDE Group entity expressing a qualified opinion on, or including an emphasis of matter in, its opinion on the statutory accounts of that FDE entity;

in each case which the Authority reasonably believes (or would be likely reasonably to believe) could directly impact on the continued performance and delivery of the Services in accordance with this Contract; and

* + 1. any [one] of the Financial Indicators set out at Paragraph 5 for any of the FDE Group entities failing to meet the required Financial Target Threshold.

1. Consequences of Financial Distress Events
   1. Immediately upon notification by the Supplier of a Financial Distress Event (or if the Authority becomes aware of a Financial Distress Event without notification and brings the event to the attention of the Supplier), the Supplier shall have the obligations and the Authority shall have the rights and remedies as set out in Paragraphs 4.3 to 4.5.
   2. In the event of a late or non-payment of a Key Sub-contractor pursuant to Paragraph 3.1.5, the Authority shall not exercise any of its rights or remedies under Paragraph 4.3 without first giving the Supplier 10 Working Days to:
      1. rectify such late or non-payment; or
      2. demonstrate to the Authority’s reasonable satisfaction that there is a valid reason for late or non-payment.
   3. The Supplier shall (and shall procure that any Monitored Supplier, the Guarantor and/or any relevant Key Sub-contractor shall):
      1. at the request of the Authority, meet the Authority as soon as reasonably practicable (and in any event within 3 Working Days of the initial notification (or awareness) of the Financial Distress Event or such other period as the Authority may permit and notify to the Supplier in writing) to review the effect of the Financial Distress Event on the continued performance and delivery of the Services in accordance with this Contract; and
      2. where the Authority reasonably believes (taking into account the discussions and any representations made under Paragraph 4.3.1 that the Financial Distress Event could impact on the continued performance and delivery of the Services in accordance with this Contract:
         1. submit to the Authority for its approval, a draft Financial Distress Remediation Plan as soon as reasonably practicable (and in any event, within 10 Working Days of the initial notification (or awareness) of the Financial Distress Event or such other period as the Authority may permit and notify to the Supplier in writing); and
         2. to the extent that it is legally permitted to do so and subject to Paragraph 4.7, provide such information relating to the Supplier, any Monitored Supplier, Key Sub-contractors and/or the Guarantor as the Authority may reasonably require in order to understand the risk to the Services, which may include forecasts in relation to cash flow, orders and profits and details of financial measures being considered to mitigate the impact of the Financial Distress Event.
   4. The Authority shall not withhold its approval of a draft Financial Distress Remediation Plan unreasonably. If the Authority does not approve the draft Financial Distress Remediation Plan, it shall inform the Supplier of its reasons and the Supplier shall take those reasons into account in the preparation of a further draft Financial Distress Remediation Plan, which shall be resubmitted to the Authority within 5 Working Days of the rejection of the first draft. This process shall be repeated until the Financial Distress Remediation Plan is either:
      1. approved by the Authority;
      2. referred, by notice sent by either Party to the other Party explaining why it thinks the Financial Distress Remediation Plan has not been approved, to commercial negotiation led by senior representatives who have authority to agree the Financial Distress Remediation Plan to be held within 28 days of the date of the notice; or
      3. finally rejected by the Authority.
   5. Following approval of the Financial Distress Remediation Plan by the Authority, the Supplier shall:
      1. on a regular basis (which shall not be less than fortnightly):
         1. review and make any updates to the Financial Distress Remediation Plan as the Supplier may deem reasonably necessary and/or as may be reasonably requested by the Authority, so that the plan remains adequate, up to date and ensures the continued performance and delivery of the Services in accordance with this Contract; and
         2. provide a written report to the Authority setting out its progress against the Financial Distress Remediation Plan, the reasons for any changes made to the Financial Distress Remediation Plan by the Supplier and/or the reasons why the Supplier may have decided not to make any changes;
      2. where updates are made to the Financial Distress Remediation Plan in accordance with Paragraph 4.5.1, submit an updated Financial Distress Remediation Plan to the Authority for its approval, and the provisions of Paragraphs 4.4 and 4.5.1 shall apply to the review and approval process for the updated Financial Distress Remediation Plan; and
      3. comply with the Financial Distress Remediation Plan (including any updated Financial Distress Remediation Plan) and ensure that it achieves the financial and performance requirements set out in the Financial Distress Remediation Plan.
   6. Where the Supplier reasonably believes that the relevant Financial Distress Event under Paragraph 4.1 (or the circumstance or matter which has caused or otherwise led to it) no longer exists, it shall notify the Authority and the Parties may agree that the Supplier shall be relieved of its obligations under Paragraph 4.5.
   7. The Supplier shall use reasonable endeavours to put in place the necessary measures to ensure that the information specified at Paragraph 4.3.2(b) is available when required and on request from the Authority and within reasonable timescales. Such measures may include:
      1. obtaining in advance written authority from Key Sub-contractors, the Guarantor and/or Monitored Suppliers authorising the disclosure of the information to the Authority and/or entering into confidentiality agreements which permit disclosure;
      2. agreeing in advance with the Authority, Key Sub-contractors, the Guarantor and/or Monitored Suppliers a form of confidentiality agreement to be entered by the relevant parties to enable the disclosure of the information to the Authority;
      3. putting in place any other reasonable arrangements to enable the information to be lawfully disclosed to the Authority (which may include making price sensitive information available to Authority nominated personnel through confidential arrangements, subject to their consent); and
      4. disclosing the information to the fullest extent that it is lawfully entitled to do so, including through the use of redaction, anonymisation and any other techniques to permit disclosure of the information without breaching a duty of confidentiality.
2. Financial Indicators

*[Guidance: The Financial Indicators set out in the table at* *paragraph 5.1 are examples of the types of Financial Indicators that Authorities may wish to use in respect of the Supplier’s financial standing. These should be aligned with any financial standing criteria used at the Conditions of Participation of the procurement and Authorities may wish to delete or insert different indicators as appropriate. Financial Indicators may be restricted to specific key indicators rather than including all of the criteria used at the Conditions of Participation.]*

* 1. Subject to the calculation methodology set out at Annex 3 of this Schedule, the Financial Indicators and the corresponding calculations and thresholds used to determine whether a Financial Distress Event has occurred in respect of those Financial Indicators, shall be as follows:

| **Financial Indicator** | **Calculation1** | **Financial Target Threshold:** | **Monitoring and Reporting Frequency** [if different from the default position set out in Paragraph 2.3.2] |
| --- | --- | --- | --- |
| 1  [Operating Margin]  OR  [The higher of (a) the Operating Margin for the most recent 12 month period and (b) the average Operating Margin for the last two 12 month periods] | [Operating Margin = Operating Profit / Revenue] | [> [X%]] | Tested and reported [yearly / half yearly] in arrears within [120 / 90] days of each [accounting reference date / half year end] based upon figures for the 12 months ending on the relevant [accounting reference date / half year end] |
| 2  [Free Cash Flow to Net Debt Ratio]  OR  [Net Debt to EBITDA Ratio] | [Free Cash Flow to Net Debt Ratio = Free Cash Flow / Net Debt]  OR  [Net Debt to EBITDA ratio = Net Debt / EBITDA] | [> [X%]]  OR  [< [X]] times | Tested and reported [yearly / half yearly] in arrears within [120 / 90] days of each [accounting reference date / half year end] based upon [Free Cash Flow / EBITDA] for the 12 months ending on, and Net Debt at, the relevant [accounting reference date / half year end] |
| 3  [Net Debt + Net Pension Deficit to EBITDA ratio] | [Net Debt + Net Pension Deficit to EBITDA Ratio = (Net Debt + Net Pension Deficit) / EBITDA] | [< [X]] times | Tested and reported yearly in arrears within 120 days of each accounting reference date based upon EBITDA for the 12 months ending on, and the Net Debt and Net Pension Deficit at, the relevant accounting reference date |
| 4  [Net Interest Paid Cover] | [Net Interest Paid Cover = Earnings Before Interest and Tax / Net Interest Paid] | [> [X]] times | Tested and reported [yearly / half yearly] in arrears within [120 / 90] days of each [accounting reference date / half year end] based upon figures for the 12 months ending on the relevant [accounting reference date / half year end] |
| 5  [Acid Ratio] | [Acid Ratio = (Current Assets – Inventories) / Current Liabilities] | [> [X]] times | Tested and reported [yearly / half yearly] in arrears within [120 /90] days of each [accounting reference date / half year end] based upon figures at the relevant [accounting reference date / half year end] |
| 6  [Net Asset value] | [Net Asset Value = Net Assets] | [> £0] | Tested and reported [yearly / half yearly] in arrears within [120 /90] days of each [accounting reference date / half year end] based upon figures at the relevant [accounting reference date / half year end] |
| 7  [Group Exposure Ratio] | [Group Exposure / Gross Assets] | [< [X]]% | Tested and reported yearly in arrears within 120 days of each accounting reference date based upon figures at the relevant accounting reference date |
| Financial Target 8  [etc.] | [etc.] | [etc.] | [etc.] |

Key:1 – See Annex 3 of this Schedule which sets out the calculation methodology to be used in the calculation of each Financial Indicator.

* 1. Monitored Suppliers

*[Guidance: Insert details of any other entities which the Supplier is required to monitor against the Financial Indicators. These are in addition to the Supplier’s monitoring of itself, the Guarantor and the Key Sub-contractors. Not all the Financial Indicators may be applicable to a Monitored Supplier, so indicate which of those are to apply in the table below.]*

| **Monitored Supplier** | Applicable Financial Indicators  (these are the Financial Indicators from the table in Paragraph 5.1 which are to apply to the Monitored Suppliers) |
| --- | --- |
| [Entity 1 e.g. Group Member, Sub-contractor, Relevant Parent Company etc.] | [1 – Operating Margin]  [2 – etc..]  [3][4][5][6][7][8][etc..] |
| [Entity 2 e.g. Group Member, Sub-contractor, Relevant Parent Company etc.] | [1 – Operating Margin]  [2 – etc.]  [3][4][5][6][7][8][etc..] |
| [etc.] | [etc.] |

1. Termination Rights
   1. The Authority shall be entitled to terminate this Contract under Clause 31.1.2 (*Termination by the Authority*) if:
      1. the Supplier fails to notify the Authority of a Financial Distress Event in accordance with Paragraph 2.3.3;
      2. the Supplier fails to comply with any part of Paragraph 4.3;
      3. the Authority finally rejects a Financial Distress Remediation Plan (or any updated Financial Distress Remediation Plan) in accordance with Paragraphs 4.4 to 4.5.1; and/or
      4. the Supplier fails to comply with the terms of the Financial Distress Remediation Plan (or any updated Financial Distress Remediation Plan) in accordance with Paragraph 4.5.3.
2. Primacy of Credit Ratings
   1. Without prejudice to the Supplier’s obligations and the Authority’s rights and remedies under Paragraph 2, if, following the occurrence of a Financial Distress Event pursuant to any of Paragraphs 3.1.2 to 3.1.10, the Rating Agencies review and report subsequently that the credit ratings for the FDE Group entities do not drop below the relevant Credit Rating Thresholds specified for those entities in Annex 2 of this Schedule, then:
      1. the Supplier shall be relieved automatically of its obligations under Paragraphs 4.3 to 4.5; and
      2. the Authority shall not be entitled to require the Supplier to provide financial information in accordance with Paragraph 4.3.2(b).
3. Board Confirmation
   1. If this Contract has been specified as a Critical Service Contract in section 9 *(Corporate Resolution Planning)* of the Front Sheet or the Supplier is or becomes a Public Sector Dependent Supplier then, subject to Paragraph 8.4 of this Schedule, the Supplier shall within 120 days after each Accounting Reference Date or within 15 months of the previous Board Confirmation (whichever is the earlier) provide a Board Confirmation to the Authority in the form set out at Annex 4 of this Schedule, confirming that to the best of the Board’s knowledge and belief, it is not aware of and has no knowledge:
      1. that a Financial Distress Event has occurred since the later of the Effective Date or the previous Board Confirmation or is subsisting; or
      2. of any matters which have occurred or are subsisting that could reasonably be expected to cause a Financial Distress Event.
   2. The Supplier shall ensure that in its preparation of the Board Confirmation it exercises due care and diligence and has made reasonable enquiry of all relevant Supplier Personnel and other persons as is reasonably necessary to understand and confirm the position.
   3. In respect of the first Board Confirmation to be provided under this Contract, the Supplier shall provide the Board Confirmation within 15 months of the Effective Date if earlier than the timescale for submission set out in Paragraph 8.1 of this Schedule.
   4. Where the Supplier is unable to provide a Board Confirmation in accordance with Paragraphs 8.1 to 8.3 of this Schedule due to the occurrence of a Financial Distress Event or knowledge of subsisting matters which could reasonably be expected to cause a Financial Distress Event, it will be sufficient for the Supplier to submit in place of the Board Confirmation, a statement from an Authorised Financial Representative to the Authority (and where the Supplier is a Strategic Supplier, the Supplier shall send a copy of the statement to the Cabinet Office Markets and Suppliers Team) setting out full details of any Financial Distress Events that have occurred and/or the matters which could reasonably be expected to cause a Financial Distress Event.

## Annex 1: Rating Agencies and their Standard Rating System

***[Guidance: This Annex 1 sets out the standard rating scales for each of the Rating Agencies selected. The Credit Rating*** *Threshold can be referred to in* *Annex* ***2*** *either by using “Credit Rating Level 1”, “Credit Rating Level 2” etc. or by reference to the Rating Agencies’ ratings “AAA”, “AA+” etc, or both.*

*Note that this Schedule is based on long-term credit ratings issued by credit ratings agencies such as Standard and Poors, Moodys, etc. These are different to and should not be substituted for credit scores issued by credit scoring agencies such as Dun and Bradstreet, Company Watch, etc).]*

[Rating Agency 1 (e.g. Standard and Poors)]

Credit Rating Level 1 = [AAA]

Credit Rating Level 2 = [AA+]

Credit Rating Level 3 = [AA]

Credit Rating Level 4 = [AA-]

Credit Rating Level 5 = [A+]

Credit Rating Level 6 = [A]

Credit Rating Level 7 = [A-]

Credit Rating Level 8 = [BBB+]

Credit Rating Level 9 = [BBB]

Credit Rating Level 10 = [BBB-]

Etc.

[Rating Agency 2 (e.g. Moodys) ]

Credit Rating Level 1 = [Aaa]

Credit Rating Level 2 = [Aa1]

Credit Rating Level 3 = [Aa2]

Credit Rating Level 4 = [Aa3]

Credit Rating Level 5 = [A1]

Credit Rating Level 6 = [A2]

Credit Rating Level 7 = [A3]

Credit Rating Level 8 = [Baa1]

Credit Rating Level 9 = [Baa2]

Credit Rating Level 10 = [Baa3]

Etc.

[Rating Agency 3 (etc.) ]

Credit Rating Level 1 = [XXX]

Etc.

## Annex 2: Credit Ratings and Credit Rating Thresholds

*[Guidance: The Key Sub-contractors listed in* *section 6 (Notified Key Sub-contractors) of the Front Sheet should be included in this table.]*

| **Entity** | **Credit Rating (long term)**  (insert credit rating issued for the entity at the Effective Date) | **Credit Rating Threshold**  (insert the actual rating (e.g. AA-) or the Credit Rating Level (e.g. Credit Rating Level 3) |
| --- | --- | --- |
| Supplier | [Rating Agency 1] – **[insert** rating for Rating Agency 1] | [Rating Agency 1] – **[insert** threshold for Rating Agency 1] |
|  | [Rating Agency 2] – **[insert** rating for Rating Agency 2] | [Rating Agency 2] – **[insert** threshold for Rating Agency 2] |
|  | [etc.] | [etc.] |
| [Guarantor] | [Rating Agency 1] – **[insert** rating for Rating Agency 1] | [Rating Agency 1] – **[insert** threshold for Rating Agency 1] |
|  | [Rating Agency 2] – **[insert** rating for Rating Agency 2] | [Rating Agency 2] – **[insert** threshold for Rating Agency 2] |
|  | [etc.] | [etc.] |
| [Key Sub-contractor 1] | [etc.] | [etc.] |
| [Key Sub-contractor 2] | [etc.] | [etc.] |
| [etc…] | [etc.] | [etc.] |
| [Monitored Supplier 1] | [etc.] | [etc.] |
| [Monitored Supplier 2] | [etc.] | [etc.] |
| [etc…] | [etc.] | [etc.] |

## Annex 3: Calculation Methodology for Financial Indicators

*[Guidance: Amend this section as appropriate to reflect the calculation methodology for those Financial Indicators that are selected for inclusion in* *Paragraph 5.1 of this Schedule.]*

The Supplier shall ensure that it uses the following general and specific methodologies for calculating the Financial Indicators against the Financial Target Thresholds:

General methodology

1. **Terminology**: The terms referred to in this Annex are those used by UK companies in their financial statements. Where the entity is not a UK company, the corresponding items should be used even if the terminology is slightly different (for example a charity would refer to a surplus or deficit rather than a profit or loss).
2. **Groups**: Where the entity is the holding company of a group and prepares consolidated financial statements, the consolidated figures should be used.
3. **Foreign currency conversion**: Figures denominated in foreign currencies should be converted at the exchange rate in force at the relevant date for which the Financial Indicator is being calculated.
4. **Treatment of non-underlying items**: Financial Indicators should be based on the figures in the financial statements before adjusting for non-underlying items.

Specific Methodology

***[Guidance: Refer to paragraph 5.1 of this Schedule for calculations of the Financial Indicators]***

| **Financial Indicator** | Specific Methodology |
| --- | --- |
| 1  [Operating Margin] | [The elements used to calculate the Operating Margin should be shown on the face of the Income Statement in a standard set of financial statements.  Figures for Operating Profit and Revenue should exclude the entity’s share of the results of any joint ventures or Associates.  Where an entity has an operating loss (i.e. where the operating profit is negative), Operating Profit should be taken to be zero.] |
| 2  [Free Cash Flow to Net Debt Ratio] | [“Free Cash Flow” = Net Cash Flow from Operating Activities – Capital Expenditure  “Capital Expenditure” = Purchase of property, plant & equipment + purchase of intangible assets  “Net Debt” = Bank overdrafts + Loans and borrowings + Finance Leases + Deferred consideration payable – Cash and cash equivalents  The majority of the elements used to calculate the Free Cash Flow to Net Debt Ratio should be shown on the face of the Statement of Cash Flows and the Balance Sheet in a standard set of financial statements.  **Net Cash Flow from Operating Activities**: This should be stated after deduction of interest and tax paid.  **Capital expenditure**: The elements of capital expenditure may be described slightly differently but will be found under ‘Cash flows from investing activities’ in the Statement of Cash Flows; they should be limited to the purchase of fixed assets (including intangible assets) for the business and exclude acquisitions. The figure should be shown gross without any deduction for any proceeds of sale of fixed assets.  **Net Debt**: The elements of Net Debt may also be described slightly differently and should be found either on the face of the Balance Sheet or in the relevant note to the financial statements. All interest bearing liabilities (other than retirement benefit obligations) should be treated as borrowings as should, where disclosed, any liabilities (less any assets) in respect of any hedges designated as linked to borrowings (but not non-designated hedges). Borrowings should also include balances owed to other group members.  Deferred consideration payable should be included in Net Debt despite typically being non-interest bearing.  Cash and cash equivalents should include short-term financial investments shown in current assets.  Where Net debt is negative (i.e. an entity has net cash), the relevant Financial Target Threshold should be treated as having been met.] |
| OR  [Net Debt to EBITDA Ratio] | OR  [“Net Debt” = Bank overdrafts + Loans and borrowings + Finance leases + Deferred consideration payable – Cash and cash equivalents  “EBITDA” = Operating profit + Depreciation charge + Amortisation charge  The majority of the elements used to calculate the Net Debt to EBITDA Ratio should be shown on the face of the Balance sheet, Income statement and Statement of Cash Flows in a standard set of financial statements but will otherwise be found in the notes to the financial statements.  **Net Debt**: The elements of Net Debt may be described slightly differently and should be found either on the face of the Balance Sheet or in the relevant note to the financial statements. All interest bearing liabilities (other than retirement benefit obligations) should be included as borrowings as should, where disclosed, any liabilities (less any assets) in respect of any hedges designated as linked to borrowings (but not non-designated hedges). Borrowings should also include balances owed to other group members.  Deferred consideration payable should be included in Net Debt despite typically being non-interest bearing.  Cash and cash equivalents should include short-term financial investments shown in current assets.  Where Net debt is negative (i.e. an entity has net cash), the relevant Financial Target Threshold should be treated as having been met.  **EBITDA**: Operating profit should be shown on the face of the Income Statement and, for the purposes of calculating this Financial Indicator, should include the entity’s share of the results of any joint ventures or Associates. The depreciation and amortisation charges for the period may be found on the face of the Statement of Cash Flows or in a Note to the Accounts. Where EBITDA is negative, the relevant Financial Target Threshold should be treated as not having been met (unless Net Debt is also negative, in which case the relevant Financial Target Threshold should be treated as having been met).] |
| 3  [Net Debt + Net Pension Deficit to EBITDA ratio] | [“Net Debt” = Bank overdrafts + Loans and borrowings + Finance leases + Deferred consideration payable – Cash and cash equivalents  “Net Pension Deficit” = Retirement Benefit Obligations – Retirement Benefit Assets  “EBITDA” = Operating profit + Depreciation charge + Amortisation charge  The majority of the elements used to calculate the Net Debt + Net Pension Deficit to EBITDA Ratio should be shown on the face of the Balance sheet, Income statement and Statement of Cash Flows in a standard set of financial statements but will otherwise be found in the notes to the financial statements.  **Net Debt**: The elements of Net Debt may be described slightly differently and should be found either on the face of the Balance Sheet or in the relevant note to the financial statements. All interest bearing liabilities (other than retirement benefit obligations) should be included as borrowings as should, where disclosed, any liabilities (less any assets) in respect of any hedges designated as linked to borrowings (but **not** non-designated hedges). Borrowings should also include balances owed to other group members.  Deferred consideration payable should be included in Net Debt despite typically being non-interest bearing.  Cash and cash equivalents should include short-term financial investments shown in current assets.  **Net Pension Deficit**: Retirement Benefit Obligations and Retirement Benefit Assets may be shown on the face of the Balance Sheet or in the notes to the financial statements. They may also be described as pension benefits / obligations, post-employment obligations or other similar terms.  Where ‘Net Debt + Net Pension Deficit’ is negative, the relevant Financial Target Threshold should be treated as having been met.  **EBITDA**: Operating profit should be shown on the face of the Income Statement and, for the purposes of calculating this Financial Indicator, should include the entity’s share of the results of any joint ventures or Associates.  The depreciation and amortisation charges for the period may be found on the face of the Statement of Cash Flows or in a Note to the Accounts.  Where EBITDA is negative, the relevant Financial Target Threshold should be treated as not having been met (unless ‘Net Debt + Net Pension Deficit’ is also negative, in which case the relevant Financial Target Threshold should be regarded as having been met).] |
| 4  [Net Interest Paid Cover] | [“Earnings Before Interest and Tax” = Operating profit  “Net Interest Paid” = Interest paid – Interest received  Operating profit should be shown on the face of the Income Statement in a standard set of financial statements and, for the purposes of calculating this Financial Indicator, should include the entity’s share of the results of any joint ventures or Associates.  Interest received and interest paid should be shown on the face of the Cash Flow statement.  Where Net interest paid is negative (i.e. the entity has net interest received), the relevant Financial Target Threshold should be treated as having been met.] |
| 5  [Acid Ratio] | [All elements that are used to calculate the Acid Ratio are available on the face of the Balance Sheet in a standard set of financial statements.] |
| 6  [Net Asset value] | [Net Assets are shown (but sometimes not labelled) on the face of the Balance Sheet of a standard set of financial statements. Net Assets are sometimes called net worth or ‘Shareholders’ Funds’. They represent the net assets available to the shareholders. Where an entity has a majority interest in another entity in which there are also minority or non-controlling interests (i.e. where it has a subsidiary partially owned by outside investors), Net Assets should be taken inclusive of minority or non-controlling interests (as if the entity owned 100% of such entity).] |
| 7  [Group Exposure Ratio] | [“Group Exposure” = Balances owed by Group Undertakings + Contingent liabilities assumed in support of Group Undertakings  “Gross Assets” = Fixed Assets + Current Assets  **Group Exposure**: Balances owed by (i.e. receivable from) Group Undertakings are shown within Fixed assets or Current assets either on the face of the Balance Sheet or in the relevant notes to the financial statements. In many cases there may be no such balances, in particular where an entity is not a member of a group or is itself the ultimate holding company of the group.  Contingent liabilities assumed in support of Group Undertakings are shown in the Contingent Liabilities note in a standard set of financial statements. They include guarantees and security given in support of the borrowings of other group companies, often as part of group borrowing arrangements. Where the contingent liabilities are capped, the capped figure should be taken as their value. Where no cap or maximum is specified, the relevant Financial Target Threshold should automatically be regarded as not having been met.  In many cases an entity may not have assumed any contingent liabilities in support of Group Undertakings, in particular where an entity is not a member of a group or is itself the ultimate holding company of the group.  **Gross Assets**: Both Fixed assets and Current assets are shown on the face of the Balance Sheet] |
| 8  [insert additional Financial Indicators as necessary] | [Etc..] |

## Annex 4: Board Confirmation

Supplier Name:

Contract Reference Number:

The Board of Directors acknowledge the requirements set out at paragraph 8 of Schedule 14 (*Financial Distress*) and confirm that the Supplier has exercised due care and diligence and made reasonable enquiry of all relevant Supplier Personnel and other persons as is reasonably necessary to enable the Board to prepare this statement.

The Board of Directors confirms, to the best of its knowledge and belief, that as at the date of this Board Confirmation it is not aware of and has no knowledge:

* + - 1. that a Financial Distress Event has occurred since the later of the previous Board Confirmation and the Effective Date or is subsisting; or
      2. of any matters which have occurred or are subsisting that could reasonably be expected to cause a Financial Distress Event

On behalf of the Board of Directors:

Chair …………………………………

Signed …………………………………

Date …………………………………

Director …………………………………

Signed …………………………………

Date …………………………………

Schedule 15

Financial Reports and Audit Rights

# Schedule 15: Financial Reports and Audit Rights

1. Definitions
   1. In this Schedule, the following definitions shall apply:

|  |  |
| --- | --- |
| “Annual Contract Report” | the annual contract report to be provided by the Supplier to the Authority pursuant to Paragraph 1 of Part B; |
| “Audit Agents” | 1. the Authority’s internal and external auditors; 2. the Authority’s statutory or regulatory auditors; 3. the Comptroller and Auditor General, their staff and/or any appointed representatives of the National Audit Office; 4. HM Treasury or the Cabinet Office; 5. any party formally appointed by the Authority to carry out audit or similar review functions; and 6. successors or assigns of any of the above; |
| “Contract Amendment Report” | the contract amendment report to be provided by the Supplier to the Authority pursuant to Paragraph 1 of Part B; |
| “Final Reconciliation Report” | the final reconciliation report to be provided by the Supplier to the Authority pursuant to Paragraph 1 of Part B; |
| “Financial Model” | the Contract Inception Report, the latest Annual Contract Report or the latest Contract Amendment Report, whichever has been most recently approved by the Authority in accordance with Paragraph 2 of Part B; |
| “Financial Reports” | the Contract Inception Report and the reports listed in the table in Paragraph 1.1 of Part B; |
| “Financial Representative” | a reasonably skilled and experienced member of the Supplier’s staff who has specific responsibility for preparing, maintaining, facilitating access to, discussing and explaining the Open Book Data and Financial Reports; |
| “Financial Transparency Objectives” | has the meaning given in Paragraph 1 of Part A; |
| “Material Change” | a Change which:   1. materially changes the profile of the Charges; or 2. varies the total Charges payable during the Term (as forecast in the latest Financial Model) by:    1. 5% or more; or    2. £1m or more; |
| “Onerous Contract” | a contract in which the unavoidable costs of meeting the obligations under the contract exceed the economic benefits expected to be received under it, as defined under International Accounting Standard 37; |
| “Onerous Contract Report” | means a report provided by the Supplier pursuant to Paragraph 3 of Part A to this Schedule; |
| “Open Book Data” | complete and accurate financial and non-financial information which is sufficient to enable the Authority to verify the Charges already paid or payable and Charges forecast to be paid during the remainder of the Term, including details and all assumptions relating to:   1. the Supplier’s Costs broken down against each Service and/or Deliverable, including actual capital expenditure (including capital replacement costs) and the unit cost and total actual costs of all hardware and software; 2. operating expenditure relating to the provision of the Services including an analysis showing:    1. the unit costs and quantity of consumables and bought-in services;    2. manpower resources broken down into the number and grade/role of all Supplier Personnel (free of any contingency) together with a list of agreed rates against each manpower grade;    3. a list of Costs underpinning those rates for each manpower grade, being the agreed rate less the Supplier’s Profit Margin; and    4. Reimbursable Expenses; 3. Overheads; 4. all interest, expenses and any other third party financing costs incurred in relation to the provision of the Services; 5. the Supplier Profit achieved over the Term and on an annual basis; 6. confirmation that all methods of Cost apportionment and Overhead allocation are consistent with and not more onerous than such methods applied generally by the Supplier; 7. an explanation of the type and value of risk and contingencies associated with the provision of the Services, including the amount of money attributed to each risk and/or contingency; and 8. the actual Costs profile for each Service Period. |

## Part A: Financial Transparency Objectives and Open Book Data

1. Financial Transparency Objectives
   1. The Supplier acknowledges that the provisions of this Schedule are designed (inter alia) to facilitate, and the Supplier shall co-operate with the Authority in order to achieve, the following objectives:
      1. Understanding the Charges
         1. for the Authority to understand any payment sought from it by the Supplier including an analysis of the Costs, Overhead recoveries (where relevant), time spent by Supplier Personnel in providing the Services and the Supplier Profit Margin;
         2. for both Parties to be able to understand the Financial Model and Cost forecasts and to have confidence that these are based on justifiable numbers and appropriate forecasting techniques;
         3. to facilitate the use of Guaranteed Maximum Price with Target Cost pricing mechanisms (where relevant as referred to in Schedule 11 (*Charges and Invoicing*);
      2. Agreeing the impact of Change
         1. for both Parties to agree the quantitative impact of any Changes that affect ongoing costs and to identify how these could be mitigated and/or reflected in the Supplier’s Charges;
         2. for both Parties to be able to review, address issues with and re‑forecast progress in relation to the provision of the Services;
      3. Continuous improvement
         1. for the Parties to challenge each other with ideas for efficiency and improvements; and
         2. to enable the Authority to demonstrate that it is achieving value for money for the tax payer relative to current market prices,

(together the “Financial Transparency Objectives”).

1. Open Book Data
   1. The Supplier acknowledges the importance to the Authority of the Financial Transparency Objectives and the Authority’s need for complete transparency in the way in which the Charges are calculated.
   2. During the Term, and for a period of 7 years following the end of the Term, the Supplier shall:
      1. maintain and retain the Open Book Data; and
      2. disclose and allow the Authority and/or the Audit Agents access to the Open Book Data.
2. Onerous Contracts
   1. If the Supplier publicly designates the Contract as an Onerous Contract (including where the Supplier has identified the Contract as such in any published accounts or public reports and announcements), the Supplier shall promptly notify the Authority of the designation and shall prepare and deliver to the Authority within the timescales agreed by the Parties (an in any event, no later than 2 months following the publication of the designation) a draft Onerous Contract Report which includes the following:
      1. an initial root cause analysis of the issues and circumstances which may have contributed to the Contract being designated as an Onerous Contract;
      2. an initial risk analysis and impact assessment on the provision of the Services as a result of the Supplier’s designation of the Contract as an Onerous Contract;
      3. the measures which the Supplier intends to put in place to minimise and mitigate any adverse impact on the provision on the Services;
      4. details of any other options which could be put in place to remove the designation of the Contract as an Onerous Contract and/or which could minimise and mitigate any adverse impact on the provision of the Services.
   2. Following receipt of the Onerous Contract Report, the Authority shall review and comment on the report as soon as reasonably practicable and the Parties shall cooperate in good faith to agree the final form of the report, which shall be submitted to the Programme Board, such final form report to be agreed no later than 1 month following the Authority’s receipt of the draft Onerous Contract Report.
   3. The Programme Board shall meet within 14 Working Days of the final Onerous Contract Report being agreed by the Parties to discuss the contents of the report; and the Parties shall procure the attendance at the meeting of any key participants where reasonably required (including the Cabinet Office Markets and Suppliers team where the Supplier is a Strategic Supplier; representatives from any Key Sub-contractors/Monitored Suppliers; and the project’s senior responsible officers (or equivalent) for each Party).
   4. The Supplier acknowledges and agrees that the report is submitted to the Authority and Programme Board on an information only basis and the Authority and Programme Board’s receipt of and comments in relation to the report shall not be deemed to be an acceptance or rejection of the report nor shall it relieve the Supplier of any liability under this Contract. Any Changes to be agreed by the Parties pursuant to the report shall be subject to the Change Control Procedure.

## Part B: Financial Reports

1. Provision of the Financial Reports
   1. The Supplier shall provide
      1. the Contract Inception Report on or before the Effective Date; and
      2. during the Term the following financial reports to the Authority, in the frequency specified below:

| **Financial Report** | **When to be provided** |
| --- | --- |
| Contract Amendment Report | Within 1 month of a Material Change being agreed between the Supplier and the Authority |
| Quarterly Contract Report | Within 1 month of the end of each Quarter |
| Annual Contract Report | Within 1 month of the end of the Contract Year to which that report relates |
| Final Reconciliation Report | Within 6 months after the end of the Term |

* 1. The Supplier shall provide to the Authority the Financial Reports in the same software package (Microsoft Excel or Microsoft Word), layout and format as the blank templates which have been issued by the Authority to the Supplier on or before the Effective Date for the purposes of this Contract. The Authority shall be entitled to modify the template for any Financial Report by giving written notice to the Supplier, including a copy of the updated template.
  2. A copy of each Financial Report shall be held by both the Authority and the Supplier. If there is a Dispute regarding a Financial Report, the Authority’s copy of the relevant Financial Report shall be authoritative.
  3. Each Financial Report shall:
     1. be completed by the Supplier using reasonable skill and care;
     2. incorporate and use the same defined terms as are used in this Contract;
     3. quote all monetary values in pounds sterling;
     4. quote all Costs as exclusive of any VAT; and
     5. quote all Costs and Charges based on current prices.
  4. Each Annual Contract Report and the Final Reconciliation Report shall be certified by the Supplier’s Chief Financial Officer or Director of Finance (or equivalent as agreed in writing by the Authority in advance of issue of the relevant Financial Report), acting with express authority, as:
     1. being accurate and not misleading;
     2. having been prepared in conformity with generally accepted accounting principles within the United Kingdom;
     3. being a true and fair reflection of the information included within the Supplier’s management and statutory accounts; and
     4. compliant with the requirements of Paragraph 1.6.
  5. The Supplier shall:
     1. prepare each Financial Report using the same methodology as that used for the Contract Inception Report;
     2. to the extent permitted by Law, ensure that each Annual Contract Report and each Contract Amendment Report (if any) is a true and fair reflection of the Costs and Supplier Profit Margin forecast by the Supplier;
     3. to the extent permitted by Law, ensure that the Final Reconciliation Report is a true and fair reflection of the Costs; and
     4. not have any other internal financial model in relation to the Services inconsistent with the Financial Model.
  6. During the Term, and for a period of 18 months following the end of the Term, the Supplier shall make available the Financial Representative at reasonable times and on reasonable notice to answer any queries that the Authority may have on any of the Financial Reports and/or Open Book Data.
  7. If the Supplier becomes aware of the occurrence, or the likelihood of the future occurrence, of an event which will or may have a material effect on the following:
     1. the Costs incurred (or those forecast to be incurred) by the Supplier; and/or
     2. the forecast Charges for the remainder of the Term,

the Supplier shall, as soon as practicable, notify the Authority in writing of the event in question detailing the actual or anticipated effect. For the avoidance of doubt, notifications provided in accordance with this Paragraph 1.8 shall not have the effect of amending any provisions of this Contract.

1. Financial Model
   1. Following the delivery by the Supplier of each Annual Contract Report and any Contract Amendment Report:
      1. the Parties shall meet to discuss its contents within 10 Working Days of receipt (or such other period as the Parties shall agree). The Financial Representative shall attend the meeting;
      2. the Supplier shall make appropriate Supplier Personnel and advisers available to discuss any variations between the relevant Financial Report and the Contract Inception Report or immediately preceding Annual Contract Report or Contract Amendment Report (as the case may be) and to explain such variations (with reference to supporting evidence) to the satisfaction of the Authority; and
      3. the Authority shall either within 10 Working Days of the meeting referred to in Paragraph 2.1.1 notify the Supplier that:
         1. the relevant Financial Report contains errors or omissions or that further explanations or supporting information is required, in which event the Supplier shall make any necessary modifications to the Financial Report and/or supply the Authority with such supporting evidence as is required to address the Authority’s concerns within 10 Working Days of such notification and the Authority shall following receipt of such amended Financial Report and/or supporting information, approve or reject such Financial Report; or
         2. the Authority has approved the relevant Financial Report.
   2. Following approval by the Authority of the relevant Financial Report in accordance with Paragraph 2.1.3, that version shall become, with effect from the date of such approval, the current approved version of the Financial Model for the purposes of this Contract, a version of which shall be held by both the Authority and the Supplier. If there is a Dispute regarding a Financial Report, the Authority’s copy of the relevant Financial Report shall be authoritative.
   3. If the Parties are unable to reach agreement on any Financial Report within 30 Working Days of its receipt by the Authority, the matter shall be referred for determination in accordance with Schedule 19 (*Dispute Resolution Procedure*).
2. Discussion of Quarterly Contract Reports and Final Reconciliation Report
   1. Following the delivery by the Supplier of each Quarterly Contract Report, the Parties shall meet to discuss its contents within 10 Working Days of receipt (or such other period as the Parties shall agree). The Financial Representative shall attend the meeting.
   2. Following the delivery by the Supplier of the Final Reconciliation Report, the Parties shall meet to discuss its contents within 10 Working Days of receipt (or such other period as the Parties shall agree). The Financial Representative shall attend the meeting.
3. Key Sub-contractors
   1. The Supplier shall, if requested by the Authority, provide (or procure the provision of) a report or reports including the level of information set out in the Financial Reports in relation to the costs and expenses to be incurred by any of its Key Sub-contractors.
   2. Without prejudice to Paragraph 1.1 of Part C, the Supplier shall:
      1. be responsible for auditing the financial models/reports of its Key Sub-contractors and for any associated costs and expenses incurred or forecast to be incurred; and
      2. on written request by the Authority, provide the Authority or procure that the Authority is provided with:
         1. full copies of audit reports for the Key Sub-contractors. The Authority shall be entitled to rely on such audit reports; and
         2. further explanation of, and supporting information in relation to, any audit reports provided.

## Part C: Audit Rights

1. Audit Rights
   1. The Authority, acting by itself or through its Audit Agents, shall have the right during the Term and for a period of 18 months thereafter, to assess compliance by the Supplier and/or its Key Sub-contractors of the Supplier’s obligations under this Contract, including for the following purposes:
      1. to verify the integrity and content of any Financial Report;
      2. to verify the accuracy of the Charges and any other amounts payable by the Authority under this Contract (and proposed or actual variations to such Charges and payments);
      3. to verify the Costs (including the amounts paid to all Sub-contractors and any third party suppliers);
      4. to verify the Certificate of Costs and/or the Open Book Data;
      5. to verify the Supplier’s and each Key Sub-contractor’s compliance with this Contract and applicable Law;
      6. to identify or investigate actual or suspected fraud, impropriety or accounting mistakes or any breach or threatened breach of security and in these circumstances the Authority shall have no obligation to inform the Supplier of the purpose or objective of its investigations;
      7. to identify or investigate any circumstances which may impact upon the financial stability of the Supplier, the Guarantor and/or any Key Sub-contractors or their ability to perform the Services;
      8. to obtain such information as is necessary to fulfil the Authority’s obligations to supply information for parliamentary, ministerial, judicial or administrative purposes including the supply of information to the Comptroller and Auditor General;
      9. to review any books of account and the internal contract management accounts kept by the Supplier in connection with this Contract;
      10. to carry out the Authority’s internal and statutory audits and to prepare, examine and/or certify the Authority’s annual and interim reports and accounts;
      11. to enable the National Audit Office to carry out an examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Authority has used its resources;
      12. to verify the accuracy and completeness of any Management Information delivered or required by this Contract;
      13. to review any Performance Monitoring Reports and/or other records relating to the Supplier’s performance of the Services and to verify that these reflect the Supplier’s own internal reports and records;
      14. to inspect the IT Environment (or any part of it) and the wider service delivery environment (or any part of it);
      15. to review the accuracy and completeness of the Registers;
      16. to review any records created during the design and development of the Supplier System and pre-operational environment such as information relating to Testing;
      17. to review the Supplier’s quality management systems (including all relevant Quality Plans and any quality manuals and procedures);
      18. to review the Supplier’s compliance with the Standards;
      19. to inspect the Authority Assets, including the Authority’s IPRs, equipment and facilities, for the purposes of ensuring that the Authority Assets are secure and that any register of assets is up to date; and/or
      20. to review the integrity, confidentiality and security of the Government Data.
   2. Except where an audit is imposed on the Authority by a regulatory body or where the Authority has reasonable grounds for believing that the Supplier has not complied with its obligations under this Contract, the Authority may not conduct an audit of the Supplier or of the same Key Sub-contractor more than twice in any Contract Year.
   3. Nothing in this Contract shall prevent or restrict the rights of the Comptroller and/or Auditor General and/or their representatives from carrying out an audit, examination or investigation of the Supplier and/or any of the Key Sub-contractors for the purposes of and pursuant to applicable Law.
2. Conduct of Audits
   1. The Authority shall during each audit comply with those security, sites, systems and facilities operating procedures of the Supplier that the Authority deems reasonable and use its reasonable endeavours to ensure that the conduct of each audit does not unreasonably disrupt the Supplier or delay the provision of the Services.
   2. Subject to the Authority’s obligations of confidentiality, the Supplier shall on demand provide the Authority and the Audit Agents with all reasonable co-operation and assistance (and shall procure such co-operation and assistance from its Sub-contractors) in relation to each audit, including:
      1. all information requested by the Authority within the permitted scope of the audit;
      2. reasonable access to any Sites and to any equipment used (whether exclusively or non-exclusively) in the performance of the Services;
      3. access to the Supplier System; and
      4. access to Supplier Personnel.
   3. The Supplier shall implement all measurement and monitoring tools and procedures necessary to measure and report on the Supplier’s performance of the Services against the applicable Performance Indicators at a level of detail sufficient to verify compliance with the Performance Indicators.
   4. The Authority shall endeavour to (but is not obliged to) provide at least 15 Working Days’ notice of its intention to conduct an audit.
   5. The Parties agree that they shall bear their own respective costs and expenses incurred in respect of compliance with their obligations under this Paragraph 2, unless the audit identifies a material Default by the Supplier in which case the Supplier shall reimburse the Authority for all the Authority’s reasonable costs incurred in connection with the audit.
3. Use of Supplier’s Internal Audit Team
   1. As an alternative to the Authority’s right pursuant to Paragraph 1.1 to exercise an audit either itself or through its Audit Agents, the Authority may require in writing that an audit is undertaken by the Supplier’s own internal audit function for any of the purposes set out in Paragraph 1.1.
   2. Following the receipt of a request from the Authority under Paragraph 3.1 above, the Supplier shall procure that the relevant audit is undertaken as soon as reasonably practicable and that the Authority has unfettered access to:
      1. the resultant audit reports; and
      2. all relevant members of the Supplier’s internal audit team for the purpose of understanding such audit reports.
4. Response to Audits
   1. If an audit undertaken pursuant to Paragraphs 1 or 3 identifies that:
      1. the Supplier has committed a Default, the Authority may (without prejudice to any rights and remedies the Authority may have) require the Supplier to correct such Default as soon as reasonably practicable and, if such Default constitutes a Notifiable Default, to comply with the Rectification Plan Process;
      2. there is an error in a Financial Report, the Supplier shall promptly rectify the error;
      3. the Authority has overpaid any Charges, the Supplier shall pay to the Authority:
         1. the amount overpaid;
         2. interest on the amount overpaid at the applicable rate under the *Late Payment of Commercial Debts (Interest) Act 1998*, accruing on a daily basis from the date of overpayment by the Authority up to the date of repayment by the Supplier; and
         3. the reasonable costs incurred by the Authority in undertaking the audit,

the Authority may exercise its right to deduct such amount from the Charges if it prefers; and

* + 1. the Authority has underpaid any Charges, the Supplier shall not be entitled to increase the Charges paid or payable by the Authority.

Schedule 16

Anticipated Savings

# Schedule 16: Anticipated Savings

This Schedule defines the key benefit categories in which savings are anticipated.

| Ref. | Benefit Category | Indicative amount (£k) | Timescale |
| --- | --- | --- | --- |
| 1 | [E.g. - Reduction in Service Charges as Service delivery becomes more efficient and effective.  Benefit realisation is measured against [a 2020/21 baseline.] | £[amount] per annum | Contract Years [x] to [y] |
| 2 | [E.g. - Improvements in Authority staff productivity from using more flexible and agile services that match the needs of the business.  Benefits realisation is measured against a baseline of 4,000 directly employed staff in 2021/22.] | £[amount] year on year improvement ([x]% productivity increase) | Contract Years [x] to [y] |
| 3 | [E.g. - Reduced electrical power consumption arising from adoption of new low energy technology.  Benefit realisation is measured against a 2020/21 baseline.] | £[amount] per annum | Contract Years [x] to [y] |

Schedule 17

Governance

# Schedule 17: Governance

1. Definitions
   1. In this Schedule, the following definitions shall apply:

|  |  |
| --- | --- |
| “Board Member” | the initial persons appointed by the Authority and Supplier to the Boards as set out in Annex 1 and any replacements from time to time agreed by the Parties in accordance with Paragraph 3.3; |
| “Boards” | the Service Management Board, Programme Board, Change Management Board, Technical Board and Risk Management Board and “Board” shall mean any of them; |
| “Change Management Board” | the body described in Paragraph 6; |
| “Project Managers” | the individuals appointed as such by the Authority and the Supplier in accordance with Paragraph 2; |
| “Risk Management Board” | the body described in Paragraph 8; |
| “Service Management Board” | the body described in Paragraph 4; and |
| “Technical Board” | the body described in Paragraph 7. |

1. Management of the Services
   1. The Supplier and the Authority shall each appoint a project manager for the purposes of this Contract through whom the Services shall be managed at a day-to-day level.
   2. Both Parties shall ensure that appropriate resource is made available on a regular basis such that the aims, objectives and specific provisions of this Contract can be fully realised.
2. Boards

Establishment and structure of the Boards

* 1. The Boards shall be established by the Authority for the purposes of this Contract on which both the Supplier and the Authority shall be represented.
  2. In relation to each Board, the:
     1. Authority Board Members;
     2. Supplier Board Members;
     3. frequency that the Board shall meet (unless otherwise agreed between the Parties);
     4. location of the Board’s meetings; and
     5. planned start date by which the Board shall be established,

shall be as set out in Annex 1.

* 1. In the event that either Party wishes to replace any of its appointed Board Members, that Party shall notify the other in writing of the proposed change for agreement by the other Party (such agreement not to be unreasonably withheld or delayed). Notwithstanding the foregoing it is intended that each Authority Board Member has at all times a counterpart Supplier Board Member of equivalent seniority and expertise.

Board meetings

* 1. Each Party shall ensure that its Board Members shall make all reasonable efforts to attend Board meetings at which that Board Member’s attendance is required. If any Board Member is not able to attend a Board meeting, that person shall use all reasonable endeavours to ensure that:
     1. a delegate attends the relevant Board meeting in his/her place who (wherever possible) is properly briefed and prepared; and
     2. that they are debriefed by such delegate after the Board Meeting.
  2. A chairperson shall be appointed by the Authority for each Board as identified in Annex 1. The chairperson shall be responsible for:
     1. scheduling Board meetings;
     2. setting the agenda for Board meetings and circulating to all attendees in advance of such meeting;
     3. chairing the Board meetings;
     4. monitoring the progress of any follow up tasks and activities agreed to be carried out following Board meetings;
     5. ensuring that minutes for Board meetings are recorded and disseminated electronically to the appropriate persons and to all Board meeting participants within 7 Working Days after the Board meeting; and
     6. facilitating the process or procedure by which any decision agreed at any Board meeting is given effect in the appropriate manner.
  3. Board meetings shall be quorate as long as at least two representatives from each Party are present.
  4. The Parties shall ensure, as far as reasonably practicable, that all Boards shall as soon as reasonably practicable resolve the issues and achieve the objectives placed before them. Each Party shall endeavour to ensure that Board Members are empowered to make relevant decisions or have access to empowered individuals for decisions to be made to achieve this.

1. Role of the Service Management Board
   1. The Service Management Board shall be responsible for the executive management of the Services and shall:
      1. be accountable to the Programme Board for comprehensive oversight of the Services and for the senior management of the operational relationship between the Parties;
      2. report to the Programme Board on significant issues requiring decision and resolution by the Programme Board and on progress against the high level Implementation Plan;
      3. receive reports from the Project Managers on matters such as issues relating to delivery of existing Services and performance against Performance Indicators, progress against the Implementation Plan and possible future developments;
      4. review and report to the Programme Board on service management, co-ordination of individual projects and any integration issues;
      5. deal with the prioritisation of resources and the appointment of Project Managers on behalf of the Parties;
      6. consider and resolve Disputes (including Disputes as to the cause of a Delay or the performance of the Services) in the first instance and if necessary escalate the Dispute to the Programme Board; and
      7. develop operational/supplier relationship and develop and propose the relationship development strategy and ensure the implementation of the same.
2. Role of the Programme Board
   1. The Programme Board shall:
      1. provide senior level guidance, leadership and strategy for the overall delivery of the Services;
      2. be the point of escalation from the Change Management Board, the Technical Board and the Service Management Board; and
      3. carry out the specific obligations attributed to it in Paragraph 5.2.
   2. The Programme Board shall:
      1. ensure that this Contract is operated throughout the Term in a manner which optimises the value for money and operational benefit derived by the Authority and the commercial benefit derived by the Supplier;
      2. receive and review reports from the Service Management Board and review reports on technology, service and other developments that offer potential for improving the benefit that either Party is receiving, in particular value for money;
      3. determine business strategy and provide guidance on policy matters which may impact on the implementation of the Services or on any Optional Services;
      4. authorise the commissioning and initiation of, and assess opportunities for, Optional Services; and
      5. provide guidance and authorisation to the Change Management Board on relevant Changes.
3. Role of the Change Management Board
   1. The Change Management Board shall assess the impact and approve or reject all Change Requests. Changes which will have a significant impact on the Services shall be escalated to the Programme Board.
   2. The Change Management Board shall:
      1. analyse and record the impact of all Changes, specifically whether the proposed Change:
         1. has an impact on other areas or aspects of this Contract and/or other documentation relating to the Services;
         2. has an impact on the ability of the Authority to meet its agreed business needs within agreed time-scales;
         3. will raise any risks or issues relating to the proposed Change; and
         4. will provide value for money in consideration of any changes to the Financial Model, future Charges and/or Performance Indicators and Target Performance Levels;
      2. provide recommendations, seek guidance and authorisation from the Programme Board as required; and
      3. approve or reject (close) all proposed Changes.
4. Role of the Technical Board
   1. The Technical Board shall be accountable to the Programme Board for oversight of the technology used in the Supplier Solution and ensuring that technological choices are made to maximise the long term value of the Supplier Solution as a business asset of the Authority.
   2. The Technical Board shall:
      1. ensure compliance with the Standards;
      2. grant dispensations for variations from such compliance where appropriate;
      3. assure the coherence and consistency of the systems architecture for the Supplier Solution;
      4. monitor developments in new technology and reporting on their potential benefit to the Services;
      5. provide advice, guidance and information on technical issues; and
      6. assure that the technical architecture of the Supplier Solution is aligned to the Service Requirements and has sufficient flexibility to cope with future requirements of the Authority.
5. Role of the Risk Management Board
   1. The Risk Management Board shall identify and manage risks relating to the performance of the Services.
   2. The Risk Management Board shall:
      1. provide assurance to the Programme Board that risks are being effectively managed across the Services, including reporting the ‘top 5’ risks to the Programme Board on a monthly basis;
      2. identify the risks to be reported to the Programme Board via the regular risk reports;
      3. subject to the Change Control Procedure, accept or reject new risks proposed for inclusion in the Risk Register;
      4. ratify or refuse requests to close risks on the Risk Register; and
      5. identify risks relating to or arising out of the performance of the Services and provisional owners of these risks.
6. Contract Management Mechanisms
   1. Both Parties shall pro-actively manage risks attributed to them under the terms of this Contract.
   2. The Supplier shall develop, operate, maintain and amend, as agreed with the Authority, processes for:
      1. the identification and management of risks;
      2. the identification and management of issues; and
      3. monitoring and controlling project plans.
   3. The Risk Register shall be updated by the Supplier and submitted for review by the Risk Management Board.
7. Annual Review
   1. An annual review meeting shall be held throughout the Term on a date to be agreed between the Parties.
   2. The meetings shall be attended by the **[insert** role] of the Supplier and the **[insert** role] of the Authority and any other persons considered by the Authority necessary for the review.

## Annex 1: Representation and Structure of Boards

Service Management Board

|  |  |
| --- | --- |
| Authority Members of Service Management Board | [ ] [Chairperson] |
| Supplier Members of Service Management Board |  |
| Start Date for Service Management Board meetings |  |
| Frequency of Service Management Board meetings |  |
| Location of Service Management Board meetings |  |

Programme Board

|  |  |
| --- | --- |
| Authority members of Programme Board | [ ] [Chairperson] |
| Supplier members of Programme Board |  |
| Start date for Programme Board meetings |  |
| Frequency of Programme Board meetings |  |
| Location of Programme Board meetings |  |

Change Management Board

|  |  |
| --- | --- |
| Authority Members of Change Management Board | [ ] [Chairperson] |
| Supplier Members of Change Management Board |  |
| Start Date for Change Management Board meetings |  |
| Frequency of Change Management Board meetings |  |
| Location of Change Management Board meetings |  |

Technical Board

|  |  |
| --- | --- |
| Authority Members of Technical Board | [ ] [Chairperson] |
| Supplier Members of Technical Board |  |
| Start Date for Technical Board meetings |  |
| Frequency of Technical Board meetings |  |
| Location of Technical Board meetings |  |

Risk Management Board

|  |  |
| --- | --- |
| Authority Members for Risk Management Board | [ ] [Chairperson] |
| Supplier Members for Risk Management Board |  |
| Start Date for Risk Management Board meetings |  |
| Frequency of Risk Management Board meetings |  |
| Location of Risk Management Board meetings |  |

Schedule 18

Change Control Procedure

# Schedule 18: Change Control Procedure

1. Definitions
   1. In this Schedule, the following definitions shall apply:

|  |  |
| --- | --- |
| “Authority Change Manager” | the person appointed to that position by the Authority from time to time and notified in writing to the Supplier or, if no person is notified, the Authority Representative; |
| “Change Request” | a written request for a Contract Change which shall be substantially in the form of Annex 1; |
| “Change Communication” | any Change Request, Impact Assessment, Change Authorisation Note or other communication sent or required to be sent pursuant to this Schedule; |
| “Drafting Party” | the Party that will prepare two copies of a Change Authorisation Note which it shall sign and deliver to the Receiving Party for its signature; |
| “Fast-track Change” | any Contract Change which the Parties agree to expedite in accordance with Paragraph 8; |
| “Impact Assessment” | an assessment of a Change Request in accordance with Paragraph 5; |
| “Impact Assessment Estimate” | has the meaning given in Paragraph 4.3; |
| “Receiving Party” | the Party which receives a proposed Change Authorisation Note for signature pursuant to Paragraph 6.2; and |
| “Supplier Change Manager” | the person appointed to that position by the Supplier from time to time and notified in writing to the Authority or, if no person is notified, the Supplier Representative. |

1. General Principles of Change Control Procedure
   1. This Schedule sets out the procedure for dealing with Changes.
   2. Operational Changes shall be processed in accordance with Paragraph 9. If either Party is in doubt about whether a change falls within the definition of an Operational Change, then it must be processed as a Contract Change.
   3. The Parties shall deal with Contract Change as follows:
      1. either Party may request a Contract Change which they shall initiate by issuing a Change Request in accordance with Paragraph 4;
      2. unless this Contract otherwise requires, the Supplier shall assess and document the potential impact of a proposed Contract Change in accordance with Paragraph 5 before the Contract Change can be either approved or implemented;
      3. the Authority shall have the right to request amendments to a Change Request, approve it or reject it in the manner set out in Paragraph 6;
      4. the Supplier shall have the right to reject a Change Request solely in the manner set out in Paragraph 7;
      5. save as otherwise provided in this Contract, no proposed Contract Change shall be implemented by the Supplier until a Change Authorisation Note has been signed and issued by the Authority in accordance with Paragraph 6.2; and
      6. if a proposed Contract Change is a Fast-track Change, it shall be processed in accordance with Paragraph 8.
   4. To the extent that any Contract Change requires testing and/or a programme for implementation, then the Parties shall follow the procedures set out in Schedule 10 (*Testing Procedures*), and, where appropriate, the Change Authorisation Note relating to such a Contract Change shall specify Milestones and/or a Key Milestone and Milestone Date(s) in respect of such Contract Change for the purposes of such procedures.
   5. Until a Change Authorisation Note has been signed and issued in accordance with Paragraph 6.2, then:
      1. unless the Authority expressly agrees (or requires) otherwise in writing, the Supplier shall continue to supply the Services in accordance with the existing terms of this Contract as if the proposed Contract Change did not apply; and
      2. any discussions, negotiations or other communications which may take place between the Authority and the Supplier in connection with any proposed Contract Change, including the submission of any Change Communications, shall be without prejudice to each Party’s other rights under this Contract.
   6. Unless the Authority directs otherwise, the Supplier shall:
      1. within 10 Working Days of the final signature and issue of a Change Authorisation Note, deliver to the Authority a copy of this Contract updated to reflect all Contract Changes agreed in the relevant Change Authorisation Note and annotated with a reference to the Change Authorisation Note pursuant to which the relevant Contract Changes were agreed; and
      2. thereafter provide to the Authority such further copies of the updated Contract as the Authority may from time to time request.
2. Costs
   1. Subject to Paragraph 3.3:
      1. the costs of preparing each Change Request shall be borne by the Party making the Change Request; and
      2. the costs incurred by the Supplier in undertaking an Impact Assessment shall be borne by the Party making the Change Request provided that the Authority shall not be required to pay any such costs if:
         1. such costs are below £**[insert** figure];
         2. the Supplier is able to undertake the Impact Assessment by using resources already deployed in the provision of the Services; or
         3. such costs exceed those in the accepted Impact Assessment Estimate.
   2. The cost of any Contract Change shall be calculated and charged in accordance with the principles and day rates or day costs (as applicable) set out in Schedule 11 (*Charges and Invoicing*). The Supplier shall be entitled to increase the Charges only if it can demonstrate in the Impact Assessment that the proposed Contract Change requires additional resources and, in any event, any change to the Charges resulting from a Contract Change (whether the change will cause an increase or a decrease in the Charges) will be strictly proportionate to the increase or decrease in the level of resources required for the provision of the Services as amended by the Contract Change.
   3. Both Parties’ costs incurred in respect of any use of this Change Control Procedure as a result of any error or Default by the Supplier shall be paid for by the Supplier.
3. Change Request
   1. Either Party may issue a Change Request to the other Party at any time during the Term. A Change Request shall be substantially in the form of Annex 1 and state whether the Party issuing the Change Request considers the proposed Contract Change to be a Fast-track Change.
   2. If the Supplier issues the Change Request, then it shall also provide an Impact Assessment to the Authority as soon as is reasonably practicable but in any event within 10 Working Days of the date of issuing the Change Request.
   3. If the Authority issues the Change Request, then the Supplier shall provide as soon as reasonably practical and in any event within ten (10) Working Days of the date of receiving the Change Request an estimate (“Impact Assessment Estimate”) of the cost of preparing an Impact Assessment and the timetable for preparing it. The timetable shall provide for the completed Impact Assessment to be received by the Authority within 10 Working Days of acceptance of the Impact Assessment Estimate or within any longer time period agreed by the Authority.
   4. If the Authority accepts an Impact Assessment Estimate then following receipt of notice of such acceptance the Supplier shall provide the completed Impact Assessment to the Authority as soon as is reasonably practicable and in any event within the period agreed in the Impact Assessment Estimate. If the Supplier requires any clarification in relation to the Change Request before it can deliver the Impact Assessment, then it shall promptly make a request for clarification to the Authority and provided that sufficient information is received by the Authority to fully understand:
      1. The nature of the request for clarification; and
      2. The reasonable justification for the request;

the time period to complete the Impact Assessment shall be extended by the time taken by the Authority to provide that clarification. The Authority shall respond to the request for clarification as soon as is reasonably practicable.

1. Impact Assessment
   1. Each Impact Assessment shall be completed in good faith and shall include:
      1. details of the proposed Contract Change including the reason for the Contract Change; and
      2. details of the impact of the proposed Contract Change on the Services, the Optional Services (if any) and the Supplier’s ability to meet its other obligations under this Contract;
      3. any variation to the terms of this Contract that will be required as a result of that impact, including changes to:
         1. the Services Description, the Performance Indicators and/or the Target Performance Levels;
         2. the format of Government Data, as set out in the Services Description;
         3. the Milestones, Implementation Plan and any other timetable previously agreed by the Parties;
         4. other services provided by third party contractors to the Authority, including any changes required by the proposed Contract Change to the Authority’s IT infrastructure;
      4. details of the cost of implementing the proposed Contract Change;
      5. details of the ongoing costs required by the proposed Contract Change when implemented, including any increase or decrease in the Charges, any alteration in the resources and/or expenditure required by either Party and any alteration to the working practices of either Party;
      6. a timetable for the implementation, together with any proposals for the testing of the Contract Change;
      7. details of how the proposed Contract Change will ensure compliance with any applicable Change in Law; and
      8. such other information as the Authority may reasonably request in (or in response to) the Change Request.
   2. If the Contract Change involves the processing or transfer of any Personal Data outside the UK, in the event of the Personal Data being subject to UK GDPR, or the EU, in the event of the Personal Data being subject to EU GDPR, the preparation of the Impact Assessment shall also be subject to Clause 21 (*Protection of Personal Data*).
   3. Subject to the provisions of Paragraph 5.4, the Authority shall review the Impact Assessment and respond to the Supplier in accordance with Paragraph 6 within 15 Working Days of receiving the Impact Assessment, it.
   4. If the Authority receives a proposed Contract Change from the Supplier and the Authority reasonably considers that it requires further information regarding the proposed Contract Change so that it may properly evaluate the Change Request and the Impact Assessment, then within 5 Working Days of receiving the Impact Assessment, it shall notify the Supplier of this fact and detail the further information that it requires. The Supplier shall then re-issue the relevant Impact Assessment to the Authority within 10 Working Days of receiving such notification. At the Authority’s discretion, the Parties may repeat the process described in this Paragraph 5.4 until the Authority is satisfied that it has sufficient information to properly evaluate the Change Request and Impact Assessment.
   5. The calculation of costs for the purposes of Paragraphs 5.1.4 and 5.1.5 shall:
      1. be based on the Financial Model;
      2. facilitate the Financial Transparency Objectives;
      3. include estimated volumes of each type of resource to be employed and the applicable rate card;
      4. include full disclosure of any assumptions underlying such Impact Assessment;
      5. include evidence of the cost of any assets required for the Change; and
      6. include details of any new Sub-contracts necessary to accomplish the Change.
2. Authority’s Right of Approval
   1. Within 15 Working Days of receiving the Impact Assessment from the Supplier or within 10 Working Days of receiving the further information that it may request pursuant to Paragraph 5.4, the Authority shall evaluate the Change Request and the Impact Assessment and shall do one of the following:
      1. approve the proposed Contract Change, in which case the Parties shall follow the procedure set out in Paragraph 6.2;
      2. in its absolute discretion reject the Contract Change, in which case it shall notify the Supplier of the rejection. The Authority shall not reject any proposed Contract Change to the extent that the Contract Change is necessary for the Supplier or the Services to comply with any Changes in Law. If the Authority does reject a Contract Change, then it shall explain its reasons in writing to the Supplier as soon as is reasonably practicable following such rejection; or
      3. in the event that it reasonably believes that a Change Request or Impact Assessment contains errors or omissions, require the Supplier to modify the relevant document accordingly, in which event the Supplier shall make such modifications within 5 Working Days of such request. Subject to Paragraph 5.4, on receiving the modified Change Request and/or Impact Assessment, the Authority shall approve or reject the proposed Contract Change within 10 Working Days.
   2. If the Authority approves the proposed Contract Change pursuant to Paragraph 6.1 and it has not been rejected by the Supplier in accordance with Paragraph 7, then it shall inform the Supplier and, unless otherwise directed by the Authority, the Supplier shall be the Drafting Party. Following receipt by the Receiving Party of the Change Authorisation Note, it shall sign both copies and return one copy to the Drafting Party. Unless otherwise specified, on the Receiving Party's signature the Change Authorisation Note shall constitute (or, where the Authority has agreed to or required the implementation of a Change prior to signature of a Change Authorisation Note, shall constitute confirmation of) a binding variation to this Contract.
   3. If the Receiving Party does not sign the Change Authorisation Note within 10 Working Days of receipt, then the Drafting Party shall have the right to notify the Receiving Party and if the Receiving Party does not sign the Change Authorisation Note within 5 Working Days of such notification, then the Drafting Party may refer the matter to the Expedited Dispute Timetable pursuant to the Dispute Resolution Procedure.
3. Supplier’s Right of Approval
   1. Following an Impact Assessment, if:
      1. the Supplier reasonably believes that any proposed Contract Change which is requested by the Authority would:
         1. materially and adversely affect the risks to the health and safety of any person; and/or
         2. require the Services to be performed in a way that infringes any Law; and/or
      2. the Supplier demonstrates to the Authority’s reasonable satisfaction that the proposed Contract Change is technically impossible to implement and neither the Supplier Solution nor the Services Description state that the Supplier does have the technical capacity and flexibility required to implement the proposed Contract Change,

then the Supplier shall be entitled to reject the proposed Contract Change and shall notify the Authority of its reasons for doing so within 5 Working Days after the date on which it is obliged to deliver the Impact Assessment pursuant to Paragraph 4.3.

1. Fast-Track Changes
   1. The Parties acknowledge that to ensure operational efficiency there may be circumstances where it is desirable to expedite the processes set out above.
   2. If:
      1. the total number of Contract Changes in relation to which this Fast-track Change procedure has been applied does not exceed 4 in any 12 month period; and
      2. both Parties agree the value of the proposed Contract Change over the remaining Term and any period for which Termination Services may be required does not exceed £**[insert** figure] and the proposed Contract Change is not significant (as determined by the Authority acting reasonably),

then the Parties shall confirm to each other in writing that they shall use the process set out in Paragraphs 4, 5, 6 and 7 but with reduced timescales, such that any period of 15 Working Days is reduced to 5 Working Days, any period of 10 Working Days is reduced to 2 Working Days and any period of 5 Working Days is reduced to 1 Working Day.

* 1. The Parties may agree in writing to revise the parameters set out in Paragraph 8.2 from time to time or that the Fast-track Change procedure shall be used in relation to a particular Contract Change notwithstanding that the total number of Contract Changes to which such procedure is applied will then exceed 4 in a 12 month period.

1. Operational Change Procedure
   1. Any Operational Changes identified by the Supplier to improve operational efficiency of the Services may be implemented by the Supplier without following the Change Control Procedure for proposed Contract Changes provided they do not:
      1. have an impact on the business of the Authority;
      2. require a Change to this Contract;
      3. have a direct impact on use of the Services; or
      4. involve the Authority in paying any additional Charges or other costs.
   2. The Authority may request an Operational Change by submitting a written request for Operational Change (“RFOC”) to the Supplier Representative.
   3. The RFOC shall include the following details:
      1. the proposed Operational Change; and
      2. the time-scale for completion of the Operational Change.
   4. The Supplier shall inform the Authority of any impact on the Services that may arise from the proposed Operational Change.
   5. The Supplier shall complete the Operational Change by the timescale specified for completion of the Operational Change in the RFOC, and shall promptly notify the Authority when the Operational Change is completed.
2. Communications
   1. For any Change Communication to be valid under this Schedule, it must be sent to either the Authority Change Manager or the Supplier Change Manager, as applicable. The provisions of Clause 42 (*Notices*) shall apply to a Change Communication as if it were a notice.

## Annex 1: Change Request Form

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CR No.: | Title: | | | Type of change: | |
| Contract: | | | Required by date: | | |
| Action: | | Name: | | | Date: |
| Raised by: | | | | | |
| Area(s) Impacted *(optional field)*: | | | | | |
| Assigned for Impact Assessment by: | | | | | |
| Assigned for Impact Assessment to: | | | | | |
| Supplier Reference No.: | | | | | |
| Full description of requested Contract Change (Including proposed Changes to the wording of the Contract): | | | | | |
| Details of any proposed alternative scenarios: | | | | | |
| Reasons for and benefits and disadvantages of requested Contract Change: | | | | | |
| Signature of requesting Change owner: | | | | | |
| Date of Request: | | | | | |

## Annex 2: Change Authorisation Note

|  |  |  |  |
| --- | --- | --- | --- |
| CR No.: | Title: | | Date raised: |
| Contract: | Type of change: | | Required by date: |
| [Key Milestone Date: [if any] ] | | | |
| Detailed description of Contract Change for which Impact Assessment is being prepared and wording of related changes to the Contract: | | | |
| Proposed adjustment to the Charges resulting from the Contract Change: | | | |
| Details of proposed one-off additional Charges and means for determining these (e.g. fixed price basis): | | | |
| Signed on behalf of the Authority: | | Signed on behalf of the Supplier: | |
| Signature:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | Signature:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| Position:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | Position:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |

Schedule 19

Dispute Resolution Procedure

# Schedule 19: Dispute Resolution Procedure

1. Definitions
   1. In this Schedule, the following definitions shall apply:

|  |  |
| --- | --- |
| “CEDR” | the Centre for Effective Dispute Resolution of International Dispute Resolution Centre 1 Paternoster Lane, St Paul’s, London, EC4M 7BQ; |
| “Counter Notice” | has the meaning given in Paragraph 7.2; |
| “Expert” | in relation to a Dispute, a person appointed in accordance with Paragraph 6.2 to act as an expert in relation to that Dispute; |
| “Expert Determination” | determination by an Expert in accordance with Paragraph 6; |
| “Mediation Notice” | has the meaning given in Paragraph 4.2; |
| “Mediator” | the independent third party appointed in accordance with Paragraph 5.2 to mediate a Dispute; |
| “Multi-Party Dispute” | a Dispute which involves the Parties and one or more Related Third Parties; |
| “Multi-Party Dispute Representatives” | has the meaning given in Paragraph 9.6; |
| “Multi-Party Dispute Resolution Board” | has the meaning given in Paragraph 9.6; |
| “Related Third Party” | a party to:   1. another contract with the Authority or the Supplier which is relevant to this Contract; or 2. a Sub-contract; and |
| “Supplier Request” | a notice served by the Supplier requesting that the Dispute be treated as a Multi-Party Dispute, setting out its grounds for that request and specifying each Related Third Party that it believes should be involved in the Multi-Dispute Resolution Procedure in respect of that Dispute. |

1. Dispute Notices
   1. If a Dispute arises then:
      1. the Authority Representative and the Supplier Representative shall attempt in good faith to resolve the Dispute; and
      2. if such attempts are not successful within a reasonable period, not being longer than 20 Working Days, either Party may issue to the other a Dispute Notice.
   2. A Dispute Notice:
      1. shall set out:
         1. the material particulars of the Dispute;
         2. the reasons why the Party serving the Dispute Notice believes that the Dispute has arisen; and
         3. if the Party serving the Dispute Notice believes that the Dispute should be dealt with under the Expedited Dispute Timetable, the reason why; and
      2. may specify in accordance with the requirements of Paragraphs 9.2 and 9.3 that the Party issuing the Dispute Notice has determined (in the case of the Authority) or considers (in the case of the Supplier) that the Dispute is a Multi-Party Dispute, in which case Paragraph 2.3 shall apply.
   3. If a Dispute Notice specifies that the Dispute has been determined or is considered to be a Multi-Party Dispute pursuant to Paragraph 2.2.2, then:
      1. if it is served by the Authority it shall be treated as a Multi-Party Procedure Initiation Notice; and
      2. if it is served by the Supplier it shall be treated as a Supplier Request,

and in each case the provisions of Paragraph 9 shall apply.

* 1. Subject to Paragraphs 2.5 and 3.2 and so long as the Authority has not served a Multi-Party Procedure Initiation Notice in respect of the relevant Dispute, following the issue of a Dispute Notice the Parties shall seek to resolve the Dispute:
     1. first by commercial negotiation (as prescribed in Paragraph 4);
     2. then, if either Party serves a Mediation Notice, by mediation (as prescribed in Paragraph 5); and
     3. lastly by recourse to arbitration (as prescribed in Paragraph 7) or litigation (in accordance with Clause 44 (*Governing Law and Jurisdiction*)).
  2. Specific issues shall be referred to Expert Determination (as prescribed in Paragraph 6) where specified under the provisions of this Contract and may also be referred to Expert Determination where otherwise appropriate as specified in Paragraph 6.1.
  3. Unless agreed otherwise in writing, the Parties shall continue to comply with their respective obligations under this Contract regardless of the nature of the Dispute and notwithstanding any issue of a Dispute Notice or a Multi-Party Procedure Initiation Notice or proceedings under Paragraph 8 (*Urgent Relief*).

1. Expedited Dispute Timetable
   1. In exceptional circumstances where the use of the times in this Schedule would be unreasonable, including (by way of example) where one Party would be materially disadvantaged by a delay in resolving the Dispute, the Parties may agree to use the Expedited Dispute Timetable. If the Parties are unable to reach agreement on whether to use the Expedited Dispute Timetable within 5 Working Days of the issue of a Dispute Notice, the use of the Expedited Dispute Timetable shall be at the sole discretion of the Authority.
   2. If the Expedited Dispute Timetable is to be used pursuant to the provisions of Paragraph 3.1 or is otherwise specified under the provisions of this Contract, then the following periods of time shall apply in lieu of the time periods specified in the applicable Paragraphs:
      1. in Paragraph 4.2.3, 10 Working Days;
      2. in Paragraph 5.2, 10 Working Days;
      3. in Paragraph 6.2, 5 Working Days; and
      4. in Paragraph 7.2, 10 Working Days.
   3. If at any point it becomes clear that an applicable deadline cannot be met or has passed, the Parties may (but shall be under no obligation to) agree in writing to extend the deadline. If the Parties fail to agree within 2 Working Days after the deadline has passed, the Authority may set a revised deadline provided that it is no less than 5 Working Days before the end of the period of time specified in the applicable Paragraphs (or 2 Working Days in the case of Paragraph 6.2). Any agreed extension shall have the effect of delaying the start of the subsequent stages by the period agreed in the extension. If the Authority fails to set such a revised deadline then the use of the Expedited Dispute Timetable shall cease and the normal time periods shall apply from that point onwards.
2. Commercial Negotiation
   1. Following the service of a Dispute Notice, then, so long as the Authority has not served a Multi-Party Procedure Initiation Notice in respect of the relevant Dispute, the Authority and the Supplier shall make reasonable endeavours to resolve the Dispute as soon as possible by commercial negotiation between the Authority’s **[insert** role] and the Supplier’s **[insert** role].
   2. If:
      1. either Party is of the reasonable opinion that the resolution of a Dispute by commercial negotiation, or the continuance of commercial negotiation, will not result in an appropriate solution;
      2. the Parties have already held discussions of a nature and intent (or otherwise were conducted in the spirit) that would equate to the conduct of commercial negotiation in accordance with this Paragraph 4; or
      3. the Parties have not settled the Dispute in accordance with Paragraph 4.1 within 30 Working Days of service of the Dispute Notice,

either Party may serve a written notice to proceed to mediation in accordance with Paragraph 5 (a “Mediation Notice”).

1. Mediation
   1. If a Mediation Notice is served, the Parties shall attempt to resolve the dispute in accordance with the version of CEDR’s Model Mediation Procedure which is current at the time the Mediation Notice is served (or such other version as the Parties may agree).
   2. If the Parties are unable to agree on the joint appointment of an independent person to mediate the Dispute within 20 Working Days from (and including) the service of a Mediation Notice then either Party may apply to CEDR to nominate such a person.
   3. If the Parties are unable to reach a settlement in the negotiations at the mediation, and only if both Parties so request and the Mediator agrees, the Mediator shall produce for the Parties a non-binding recommendation on terms of settlement. This shall not attempt to anticipate what a court might order but shall set out what the Mediator suggests are appropriate settlement terms in all of the circumstances.
   4. Any settlement reached in the mediation shall not be legally binding until it has been reduced to writing and signed by, or on behalf of, the Parties (in accordance with the Change Control Procedure where appropriate). The Mediator shall assist the Parties in recording the outcome of the mediation.
2. Expert Determination
   1. If a Dispute relates to any aspect of the technology underlying the provision of the Services or otherwise relates to a technical matter of an IT, accounting or financing nature and the Dispute has not been resolved by commercial negotiation in accordance with Paragraph 4 or, if applicable, mediation in accordance with Paragraph 5, then either Party may by written notice to the other request (agreement to which request shall not be unreasonably withheld or delayed) that the Dispute be referred to an Expert for determination.
   2. The Expert shall be appointed by agreement in writing between the Parties, but in the event of a failure to agree within 10 Working Days of the relevant request made pursuant to Paragraph 6.1, or if the person appointed is unable or unwilling to act, the Expert shall be appointed:
      1. if the Dispute relates to any aspect of the technology underlying the provision of the Services or a matter of an IT technical nature, on the instructions of the President of the British Computer Society (or any other association that has replaced the British Computer Society);
      2. if the Dispute relates to a matter of a financial technical nature, on the instructions of the President of the Institute of Chartered Accountants of England and Wales; or
      3. if the Dispute relates to a matter of a technical nature not falling within Paragraphs 6.2.1 or 6.2.2, on the instructions of the president (or equivalent) of:
         1. an appropriate body agreed between the Parties; or
         2. if the Parties do not reach agreement on the relevant body within 15 Working Days of the relevant request made pursuant to Paragraph 6.1, such body as may be specified by the President of the Law Society on application by either Party.
   3. The Expert shall act on the following basis:
      1. they shall act as an expert and not as an arbitrator and shall act fairly and impartially;
      2. the Expert’s determination shall (in the absence of a material failure to follow the agreed procedures) be final and binding on the Parties;
      3. the Expert shall decide the procedure to be followed in the determination and shall be requested to make his/her determination within 30 Working Days of his appointment or as soon as reasonably practicable thereafter and the Parties shall assist and provide the documentation that the Expert requires for the purpose of the determination;
      4. any amount payable by one Party to another as a result of the Expert’s determination shall be due and payable within 20 Working Days of the Expert’s determination being notified to the Parties;
      5. the process shall be conducted in private and shall be confidential; and
      6. the Expert shall determine how and by whom the costs of the determination, including his/her fees and expenses, are to be paid.
3. Arbitration
   1. Subject to compliance with its obligations under Paragraph 4.1 and to the provisions of Paragraph 6, the Authority may at any time before court proceedings are commenced refer the Dispute to arbitration in accordance with the provisions of Paragraph 7.5.
   2. Before the Supplier commences court proceedings or arbitration, it shall serve written notice on the Authority of its intentions and the Authority shall have 15 Working Days following receipt of such notice to serve a reply (a “Counter Notice”) on the Supplier requiring the Dispute to be referred to and resolved by arbitration in accordance with Paragraph 7.5 or be subject to the exclusive jurisdiction of the courts of England and Wales. The Supplier shall not commence any court proceedings or arbitration until the expiry of such 15 Working Day period.
   3. If the Authority serves a Counter Notice, then:
      1. if the Counter Notice requires the Dispute to be referred to arbitration, the provisions of Paragraph 7.5 shall apply; or
      2. if the Counter Notice requires the Dispute to be subject to the exclusive jurisdiction of the courts of England and Wales, the Dispute shall be so referred to those courts and the Supplier shall not commence arbitration proceedings.
   4. If the Authority does not serve a Counter Notice within the 15 Working Day period referred to in Paragraph 7.2, the Supplier may either commence arbitration proceedings in accordance with Paragraph 7.5 or commence court proceedings in the Courts of England and Wales which shall (in those circumstances) have exclusive jurisdiction.
   5. The Parties hereby confirm that if any arbitration proceedings are commenced pursuant to Paragraphs 7.1 to 7.4:
      1. the Dispute shall be referred to and finally resolved by arbitration under the Rules of the London Court of International Arbitration (“LCIA”) (subject to Paragraphs 7.5.5, 7.5.6 and 7.5.7);
      2. the arbitration shall be administered by the LCIA;
      3. the LCIA procedural rules in force at the date that the Dispute was referred to arbitration shall be applied and are deemed to be incorporated by reference into this Contract and the decision of the arbitrator shall be binding on the Parties in the absence of any material failure to comply with such rules;
      4. if the Parties fail to agree the appointment of the arbitrator within 10 Working Days from the date on which arbitration proceedings are commenced or if the person appointed is unable or unwilling to act, the arbitrator shall be appointed by the LCIA;
      5. the chair of the arbitral tribunal shall be British;
      6. the arbitration proceedings shall take place in London and in the English language; and
      7. the seat of the arbitration shall be London.
4. Urgent Relief
   1. Either Party may at any time take proceedings or seek remedies before any court or tribunal of competent jurisdiction:
      1. for interim or interlocutory remedies in relation to this Contract or infringement by the other Party of that Party’s Intellectual Property Rights; and/or
      2. where compliance with Paragraph 2.1 and/or referring the Dispute to mediation may leave insufficient time for that Party to commence proceedings before the expiry of the limitation period.
5. Multi-Party Disputes
   1. All Multi-Party Disputes shall be resolved in accordance with the procedure set out in this Paragraph 9 (the “Multi-Party Dispute Resolution Procedure”).
   2. If at any time following the issue of a Dispute Notice, the Authority reasonably considers that the matters giving rise to the Dispute involve one or more Related Third Parties, then the Authority shall be entitled to determine that the Dispute is a Multi-Party Dispute and to serve a notice on the Supplier which sets out the Authority’s determination that the Dispute is a Multi-Party Dispute and specifies the Related Third Parties which are to be involved in the Multi-Party Dispute Resolution Procedure, such notice a “Multi-Party Procedure Initiation Notice”.
   3. If following the issue of a Dispute Notice but before the Dispute has been referred to Expert Determination or to arbitration in accordance with Paragraph 7, the Supplier has reasonable grounds to believe that the matters giving rise to the Dispute have been contributed to by one or more Related Third Parties, the Supplier may serve a Supplier Request on the Authority.
   4. The Authority shall (acting reasonably) consider each Supplier Request and shall determine within 5 Working Days whether the Dispute is:
      1. a Multi-Party Dispute, in which case the Authority shall serve a Multi-Party Procedure Initiation Notice on the Supplier; or
      2. not a Multi-Party Dispute, in which case the Authority shall serve written notice of such determination upon the Supplier and the Dispute shall be treated in accordance with Paragraphs 3 to 8.
   5. If the Authority has determined, following a Supplier Request, that a Dispute is not a Multi-Party Dispute, the Supplier may not serve another Supplier Request with reference to the same Dispute.
   6. Following service of a Multi-Party Procedure Initiation Notice a Multi-Party Dispute shall be dealt with by a board (in relation to such Multi-Party Dispute, the “Multi-Party Dispute Resolution Board”) comprising representatives from the following parties to the Multi-Party Dispute, each of whom shall be of a suitable level of seniority to finalise any agreement with the other parties to settle the Multi-Party Dispute:
      1. the Authority;
      2. the Supplier;
      3. each Related Third Party involved in the Multi-Party Dispute; and
      4. any other representatives of any of the Parties and/or any Related Third Parties whom the Authority considers necessary,

(together “Multi-Party Dispute Representatives”).

* 1. The Parties agree that the Multi-Party Dispute Resolution Board shall seek to resolve the relevant Multi-Party Dispute in accordance with the following principles and procedures:
     1. the Parties shall procure that their Multi-Party Dispute Representatives attend, and shall use their best endeavours to procure that the Multi-Party Dispute Representatives of each Related Third Party attend, all meetings of the Multi-Party Dispute Resolution Board in respect of the Multi-Party Dispute;
     2. the Multi-Party Dispute Resolution Board shall first meet within 10 Working Days of service of the relevant Multi-Party Procedure Initiation Notice at such time and place as the Parties may agree or, if the Parties do not reach agreement on the time and place within 5 Working Days of service of the relevant Multi-Party Procedure Initiation Notice, at the time and place specified by the Authority, provided such place is at a neutral location within England and that the meeting is to take place between 9.00am and 5.00pm on a Working Day; and
     3. in seeking to resolve or settle any Multi-Party Dispute, the members of the Multi-Party Dispute Resolution Board shall have regard to the principle that a Multi-Party Dispute should be determined based on the contractual rights and obligations between the Parties and the Related Third Parties and that any apportionment of costs should reflect the separate components of the Multi-Party Dispute.
  2. If a Multi-Party Dispute is not resolved between the Parties and all Related Third Parties within 25 Working Days of the issue of the Multi-Party Procedure Initiation Notice (or such longer period as the Parties may agree in writing), then:
     1. either Party may serve a Mediation Notice in respect of the Multi-Party Dispute in which case Paragraph 5 shall apply;
     2. either Party may request that the Multi-Party Dispute is referred to an Expert in which case Paragraph 6 shall apply; and/or
     3. subject to Paragraph 9.9, Paragraph 7 shall apply to the Multi-Party Dispute,

and in each case references to the “Supplier” or the “Parties” in such provisions shall include a reference to all Related Third Parties.

* 1. If a Multi-Party Dispute is referred to arbitration in accordance with Paragraph 7 or a Dispute becomes a Multi-Party Dispute during the course of arbitration proceedings and either Party is unable to compel a Related Third Party to submit to such arbitration proceedings, the Authority or the Supplier may discontinue such arbitration proceedings and instead initiate court proceedings. The costs of any such discontinued arbitration proceedings shall be borne by the Party which is in a direct contractual relationship with the Related Third Party or, where the Related Third Party is a Sub Contractor, by the Supplier.

Schedule 20

Reports and Records Provisions

# Schedule 20: Reports and Records Provisions

1. Other Reports
   1. The Authority may require any or all of the following reports:
      1. delay reports;
      2. reports relating to Testing and tests carried out under Schedule 5 (*Security Management*) and Schedule 22 (*Service Continuity Plan and Corporate Resolution Planning*);
      3. reports which the Supplier is required to supply as part of the Management Information;
      4. annual reports on the Insurances;
      5. security reports; and
      6. Force Majeure Event reports.
2. Records
   1. The Supplier shall retain and maintain all the records (including superseded records) referred to in Paragraph 1 and Annex 1 (together “Records”):
      1. in accordance with the requirements of The National Archives and Good Industry Practice;
      2. in chronological order;
      3. in a form that is capable of audit; and
      4. at its own expense.
   2. The Supplier shall make the Records available for inspection to the Authority on request, subject to the Authority giving reasonable notice.
   3. Where Records are retained in electronic form, the original metadata shall be preserved together with all subsequent metadata in a format reasonably accessible to the Authority.
   4. The Supplier shall, during the Term and a period of at least 7 years following the expiry or termination of this Contract, maintain or cause to be maintained complete and accurate documents and records in relation to the provision of the Services including but not limited to all Records.
   5. Records that contain financial information shall be retained and maintained in safe storage by the Supplier for a period of at least 7 years after the expiry or termination of this Contract.
   6. Without prejudice to the foregoing, the Supplier shall provide the Authority:
      1. as soon as they are available, and in any event within 60 Working Days after the end of the first 6 months of each financial year of the Supplier during the Term, a copy, certified as a true copy by an authorised representative of the Supplier, of its un-audited interim accounts and, if applicable, of consolidated un-audited interim accounts of the Supplier and its Affiliates which would (if the Supplier were listed on the London Stock Exchange (whether or not it is)) be required to be sent to shareholders as at the end of and for each such 6 month period; and
      2. as soon as they shall have been sent to its shareholders in order to be laid before an annual general meeting of the Supplier, but not later than 130 Working Days after the end of each accounting reference period of the Supplier part or all of which falls during the Term, the Supplier’s audited accounts and if applicable, of the consolidated audited accounts of the Supplier and its Affiliates in respect of that period together with copies of all related directors’ and auditors’ reports and all other notices/circulars to shareholders.
3. Virtual Library
   1. The Supplier shall, no later than eight (8) weeks prior to the Operational Service Commencement Date and without charge to the Authority, create a Virtual Library on which the Supplier shall (subject to any applicable legislation governing the use or processing of personal data) make information about this Contract available in in accordance with the requirements outlined in this Schedule.
   2. The Supplier shall ensure that the Virtual Library is:
      1. capable of holding and allowing access to the information described in Annex 2 of this Schedule and includes full and accurate file details of all uploaded items including date and time of upload, version number and the name of the uploader;
      2. structured so that each document uploaded has a unique identifier which is automatically assigned;
      3. readily accessible by the Authority at all times in full via a user-friendly, password protected interface to such nominated users as are notified to the Supplier by the Authority from time to time,
      4. structured so as to allow nominated users to download either specific documents or the complete Virtual Library (to the extent it has Access Permission) in bulk and store and view the content offline (on a regular and automated basis);
      5. structured and maintained in accordance with the security requirements as set out in this Contract including those set out in Schedule 5 (*Security Management*);
      6. created and based on open standards in Schedule 4 (*Standards*); and
      7. backed up on a secure off-site system.
   3. For the avoidance of doubt, the Virtual Library (excluding any Software used to host it) shall form a database which constitute Project Specific IPR which shall be assigned to the Authority pursuant to Schedule 27 (*Intellectual Property Rights*) of this Contract.
   4. The Supplier shall upload complete and accurate information specified in Annex 2 by the Initial Upload Date (except where prior to the launch of the Virtual Library in which case the date at which the Virtual Library is made available in accordance with Paragraph 3.1) onto Virtual Library in the format specified.
   5. Upon any document being uploaded to the Virtual Library, and where the Authority has been granted Access Permission to that document, the Supplier shall email on the same date as the upload, a copy of the document to the nominated Authority email address at:

[ ]

* 1. Except for notices under Clause 42.1 or items covered by Clause 42.4, where the Supplier is under an obligation to provide information to the Authority in a provision under this Contract, then the Supplier’s upload of that information onto the Virtual Library shall satisfy the Supplier’s obligation to provide the Authority with that information provided that the Authority has access in accordance with this Paragraph 3 and the uploaded information meets the requirements more particularly specified in the relevant provision.
  2. Except to the extent that the requirements provide for earlier and more regular Authority access to up-to-date information, Annex 2 shall not take precedence over any other obligation to provide information in this Contract and the Supplier shall refer to the applicable clause for further details as to the requirement.
  3. The Supplier shall provide each specified person (as set out in column 6 of the table at Annex 2) access to view and download the specified information in the Virtual Library in Annex 2 subject upon the occurrence of the event specified in the column marked Access Permission in Annex 2 to this Schedule.
  4. Where Access Permission is not listed (in column 6 of the table at Annex 2) as being subject to the occurrence of a certain event the Supplier shall grant access to the person and information specified (in column 6 of the table at Annex 2) from the Initial Upload Date.
  5. Where Access Permission is specified as being granted to the Authority’s Third Party Auditor (prior to the Authority being granted access) it shall:
     1. be entitled to access, view and download information specified in Annex 2 subject to it entering into a confidentiality agreement with the Supplier to keep the contents confidential (except to the extent disclosure of the confidential information is required under Paragraph 3.10.2 of this Schedule); and
     2. report to the Authority (at its request) as to the completeness and accuracy of the information but not the substance of the information.
  6. The Supplier shall ensure that the Virtual Library retains in an accessible form all historic or superseded records of the information specified Annex 2. In order to maintain the integrity of the historic archive of the information and documentation and for the purposes of maintaining a clear audit trail, the Supplier shall not delete or overwrite any information that has been stored in the Virtual Library, except for the purposes of maintenance (provided no information is lost during maintenance) or to enable the Supplier to comply with Data Protection Legislation.
  7. The Supplier warrants that the information uploaded to the Virtual Library is accurate, complete, up-to-date and in accordance with this Contract at the date of upload.
  8. Where the Supplier becomes aware that any of the information provided on the Virtual Library is materially inaccurate, incomplete or out of date (other than in respect of historic versions of documents) the Supplier shall provide an update to the information within fourteen (14) days unless already due to be updated beforehand due to an Update Requirement specified in Annex 2.
  9. In the event of a conflict between any requirement in this Contract (excluding Annex 2) for the Supplier to provide information to the Authority and the requirements set out in Annex 2 of this Schedule, the requirement elsewhere in this Contract shall prevail.
  10. The Supplier shall ensure that all approved users of the Virtual Library are alerted by email each time that information in the Virtual Library is uploaded or updated as it occurs.
  11. No later than one (1) Month prior to the Operational Service Commencement Date, the Supplier shall provide training manuals to the Authority relating to the use of the Virtual Library.
  12. On request by the Authority the Supplier shall provide the Authority’s nominated users with a reasonable level of training and ongoing support to enable them to make use of the Virtual Library.
  13. For the avoidance of doubt, the cost of any redactions, access restrictions or compliance with the Data Protection Legislation in respect of the information hosted on the Virtual Library shall be at the Supplier’s own cost and expense.

## Annex 1: Records to be Kept by the Supplier

The records to be kept by the Supplier are:

1. This Contract, its Schedules and all amendments to such documents.
2. All other documents which this Contract expressly requires to be prepared.
3. Records relating to the appointment and succession of the Supplier Representative and each member of the Key Personnel.
4. Notices, reports and other documentation submitted by any Expert.
5. All operation and maintenance manuals prepared by the Supplier for the purpose of maintaining the provision of the Services and the underlying IT Environment and Supplier Equipment.
6. Documents prepared by the Supplier or received by the Supplier from a third party relating to a Force Majeure Event.
7. All formal notices, reports or submissions made by the Supplier to the Authority Representative in connection with the provision of the Services.
8. All certificates, licences, registrations or warranties in each case obtained by the Supplier in relation to the provision of the Services.
9. Documents prepared by the Supplier in support of claims for the Charges.
10. Documents submitted by the Supplier pursuant to the Change Control Procedure.
11. Documents submitted by the Supplier pursuant to invocation by it or the Authority of the Dispute Resolution Procedure.
12. Documents evidencing any change in ownership or any interest in any or all of the shares in the Supplier and/or the Guarantor, where such change may cause a change of Control; and including documents detailing the identity of the persons changing such ownership or interest.
13. Invoices and records related to VAT sought to be recovered by the Supplier.
14. Financial records, including audited and un-audited accounts of the Guarantor and the Supplier.
15. Records required to be retained by the Supplier by Law, including in relation to health and safety matters and health and safety files and all consents.
16. All documents relating to the insurances to be maintained under this Contract and any claims made in respect of them.
17. All journals and audit trail data referred to in Schedule 5 (*Security Management*).
18. All other records, notices or certificates required to be produced and/or maintained by the Supplier pursuant to this Contract.

## Annex 2: Records to Upload to Virtual Library

***[Guidance:******This Annex 2 is an example template and currently includes a list of some of the information already required under the Contract which is required to be maintained in the Virtual Library by the Supplier. The Authority will need to update this table to reflect the requirements of the particular procurement and any changes which the Authority has made to the drafting elsewhere in the Contract in respect of any of the information listed here and will need to consider Access Permissions and Access Events for each item of information listed, depending on the nature of the information.]***

| **Applicable Clause/ Paragraph** | **Required Data** | **Format of Data** | **Initial Upload Date** | **Update Requirement** | **Access Permission and Access Event (where applicable)** |
| --- | --- | --- | --- | --- | --- |
| Cl. 5.5.5, 5.5.6, 5.8.2 | Documentation | As appropriate and agreed by the Authority | Within seven (7) days of the issue of a Milestone Achievement Certificate in respect of the relevant Deliverable. | - | Authority |
| Cl 6.4 | Detailed Implementation Plan | Sch 9 | Within 20 Working Days of Effective Date | Every 3 months from Effective Date | Authority |
| Cl 33.8.8 | Annual slavery and human trafficking report | As appropriate and agreed by the Authority | Within twelve (12) months | Every twelve (12) months | Authority |
| Cl 14.3 | Key Personnel | Section 11 of the Front Sheet | Effective Date | On replacement of Key Personnel | Authority |
| Cl 15.7 | Notified Key Subcontractors | Section 6 of the Front Sheet | Effective Date | On replacement of key subcontractor | Authority |
| Cl 15.6 and 15.7 | Notified Key Sub-Contractors | Section 6 *(Notified Key Sub-contractors)* of the Front Sheet | Effective Date | With each approved appointment or variation | Authority |
| Sch 3, Part B Para 2.3 | Performance Monitoring Report and the Balanced Sustainability Report | Sch 3, Part B | Service Commencement | Within ten (10) Working Days of the end of each Service Period | Authority |
| Sch 4, Annex 1, Para 4 | Evidence of compliance with sustainability requirements | - | On reasonable request by Authority, provided that such requests are limited to [2] per Contract Year | On reasonable request by Authority, provided that such requests are limited to [2] per Contract Year | Authority |
| Sch 4, Annex 1, Para 4 | Sustainability Report | Sch 4, Annex 1, Table C | As set out in Table C | As set out in Table C | Authority |
| Sch 5, Para 14, 15, and 16 | Security Management Plan | Sch 5, Para 14, 15 and 16 | As set out in Sch 5, Para 14, 15 and 16 | Regular review and at least annually | Authority |
| Sch 5, Para 13 | Relevant Certifications | Sch 5, Para 13 | Before Supplier begins to provide the Services | - | - |
| Sch 5, Para 11 | Diagram documenting the Supplier Information Management System, the Wider Information Management System and the boundary between them | Sch 5, Para 11 | The date specified in the Detailed Implementation Plan | Regular review and at least annually | Authority |
| Sch 6, Para 4 | Evidence of Insurances | Sch 6 | Effective Date | Within fifteen (15) days after policy renewal or replacement | Authority |
| Section 5 of the Front Sheet | Commercially Sensitive Information | Section 5 of the Front Sheet | Effective Date | Upon Agreement by the Authority to vary the information | Authority and/or Auditor |
| Section 7 of the Front Sheet | Third Party Contracts | Section 7 of the Front Sheet | Effective Date | On appointment of subcontract | Authority |
| Section 8 of the Front Sheet | Supplier Software and Third Party Software | Section 8 of the Front Sheet | Effective Date | No less than every 6 (six) Months from the Effective Date | Authority |
| Sch 10, Para 4 | Test Strategy | As appropriate and agreed by the Authority | Within 20 Working Days of Effective Date | Upon update to the test strategy | Authority |
| Sch 10, Para 5 | Test Plan | As appropriate and agreed by the Authority | 20 prior Working Days of relevant test | Upon update to the test plan | Authority |
| Sch 10, Para 8 | Test Specification | As appropriate and agreed by the Authority | 10 prior Working Days of relevant test | Upon update to the test specification | Authority |
| Sch 10, Para 8 | Test Report | As appropriate and agreed by the Authority | 2 Working Days prior to the date on which the test is planned to end for the Draft Test Report  5 days for the Final Test Report following the relevant test completion | Reissue with each retest | Authority |
| Sch 11, Part E, Para 1.1 | Template Invoice | As appropriate and agreed by the Authority | Within 10 Working Days of the Effective Date | Upon Agreement by the Authority to vary the template | Authority |
| Sch 11, Annex 4 | Risk Register | Sch 11, Annex 4 | Effective Date | Upon Agreement by the Authority to vary the by the Risk Management Board | Authority |
| Sch 13, Para 4 | Benchmarking Plan | Sch 13 | Upon receipt from Benchmarker | Approval of Plan | Authority and Auditor |
| Sch 13, Para 8 | Benchmarking report | Sch 13 | Upon receipt from Benchmarker | Any update | Authority and Auditor |
| Sch 14, Para 2.3.2 | Financial Indicator Reports | Sch 14, Para 2.5 | As specified in Para 2.3.2 of Sch 14 | As specified in Para 2.3.2 of Sch 14 | Authority |
| Sch 14 Para 4.3.2 | Financial Distress Remediation Plan | As appropriate and agreed by the Authority | As soon as reasonably practicable and in any event within 10 Working Days of initial notification or awareness of a Financial Distress Event | On a regular basis (not less than fortnightly) | Authority |
| Sch 18, Para 8 | Board Confirmation | As set out at Annex 4 of Sch 18 | Within 120 days of the first Accounting Reference Date to occur | Woithin 15 months of the previous Board Confirmation Provided or within 120 days after each Accounting Reference Date (whichever is the earlier) | Authority |
| Sch 19, Part B, Para 11.1 | Contract Amendment Report | Sch 19, Part B, Para 1.2 | Within 1 month of a material change being agreed | - | Authority |
| Sch 19, Para 1.1 | Quarterly Contract Report | Sch 19, Part B, Para 1.2 | Within 1 month of the end of each Quarter | - | Authority |
| Sch 19, Part B, Para 1.1 | Annual Contract Report | Sch 19, Part B, Para 1.2 | Within 1 month of the end of the Contract Year to which that report relates | - | Authority |
| Sch 19, Part B, Para 1.1 | Financial Reconciliation Report | Sch 19, Part B, Para 1.2 | Within 6 months after the end of the Term | - | Authority |
| Sch 17, Para 3.3 | Representation and Structure of boards | Sch 17 Annex 1 | Within 7 days of receipt of intention, or in the case of a non-Authority board member agreement by the Authority | - | Authority |
| Sch 17, Para 3.5.5 | Minutes of governance meetings (all boards) | As appropriate and agreed by the Authority | Within 7 days of receipt from chairperson | - | Authority |
| Sch 18 Para 4.3 | Impact Assessment Estimate | As appropriate and agreed by the Authority | Within 10 Working Days of date of receiving change request. | - | Authority |
| Sch 18 Para 5 | Impact Assessment | As appropriate and agreed by the Authority | Within the period agreed by the Impact Assessment Estimate | Within 10 Working Days of request by the Authority to update under Sch 18, Para 5.4 | Authority |
| Sch 18, Para 2.6 | Update full copy of the Contract and copy of annotated version illustrating changes (unless Authority directs otherwise) | PDF and MS Word (editable) | Signature of Variation Date | Any variation | Authority |
| Sch 18, Para 4 | Change Request | Sch 18, 1 | Within 10 Working Days of Authority issuing the Change Request | - | Authority |
| Sch 18, Para 6.2 | Change Authorisation Note (unless Authority directs otherwise) | Sch 18, Annex 2 | When Authority approves proposed Contract Change pursuant to Paragraph 6.1 and it has not been rejected by the Supplier in accordance with Paragraph 7 | - | Authority |
| Sch 19, Para 2.1 | Dispute Notice | Sch 19 Para 2.2 | No longer than 20 Working Days from an unresolved dispute arising | Any variation | Authority |
| Sch 19, Para 2.4 | Mediation Notice | As appropriate | When first served | Any variation | Authority |
| Sch 20, Para 1 | Reports and Records Provisions | Sch 20, Annex 1 | Within 3 months of the Effective Date | Frequency specified in Sch 20 | Authority |
| Sch 21, Para 2.1.1 | Register of All Assets, Sub-contracts and Other Relevant Agreements | As appropriate and agreed by the Authority | Within 3 months of the Effective Date | Any variation | Authority |
| Sch 21, Para 2.1.2 | Configuration Database of Technical Infrastructure and Operating Procedures | As appropriate and agreed by the Authority | Within 3 months of the Effective Date | Any variation | Authority |
| Sch 21, Para 3.1 | Exit Information | As appropriate and agreed by the Authority | On reasonable notice given by the Authority at any point during the Term | Within 10 Working Days of Authority’s written request | Authority and its potential Replacement Suppliers |
| Sch 21, Para 5.1 | Exit Plan | Sch 21, Para 5.3 | Within 3 months of the Effective Date | In the first month of each contract year; and  Within 14 days if requested by the Authority following a Financial Distress Event  Within 20 days after service of Termination Notice or 6 months prior to expiry of the Contract | Authority |
| Sch 21, Para 6.3.5 | Provide up to date Registers during the Termination Assistance Period | As appropriate | As requested by the Authority | As appropriate |  |
| Sch 21, Para 6.7.2 | Government Data (handback) | Sch 21, Para 2 and/or as appropriate and agreed by the Authority | At the end of the Termination Assistance Period | - | Authority |
| Sch 21, Annex 1, Para 1.1, Para 1.2 Para 1.3 & Para 1.4 | Termination Services supporting documentation and knowledge transfer material | As appropriate and agreed by the Authority | As specified in the Termination Assistance Notice and in any event prior to the end of the Termination Assistance Period | As specified in the Termination Assistance Notice or otherwise requested by the Authority | - |
| Sch 22 Service Continuity | Service Continuity Plan | Sch 22, Para 2.2 | Within 40 Working Days from the Effective Date | Sch 22, Para 7.1 | Authority |
| Sch 22, Para 7.2 | Service Continuity Plan Review Report | Sch 22, Para 6.2 | Within 20 Working Days of the conclusion of each review of the Service Continuity Plan. | - | - |
| Sch 22, Part B | Corporate Resolution Planning Information | Sch 22, Part B, Para 2.3 | Sch 22 Part B Para 2.2 | Sch 22, Para 2.8 | Authority |
| Sch 24, Part E, Para 1.1 | Provisional Supplier Personnel List and, Staffing Information | As appropriate and agreed by the Authority, in a suitably anonymised format so as to comply with the DPA 2018, see Annex E2 | Varies - Sch 24, Para 1.1.1 - 1.1.4 | At such intervals as are reasonably requested by the Authority | Authority |
| Sch 24, Part E, Para 1.2 | Final Supplier Personnel List | As appropriate and agreed by the Authority, see Annex E2 | At least 20 Working Days prior to the Service Transfer Date | Upon any material change to the list of employees | Authority and, at the discretion of the Authority, the prospective Replacement Supplier and/or any prospective Replacement Subcontractor |
| Sch 24, Part E, Para 1.6 | Information relating to the manner in which the services are organised | As appropriate and agreed by the Authority, see Annex E2 | Within 20 Working Days of Authority request | Within 20 Working Days of Authority request | Authority |
| Sch 24, Part E, Para 1.7 | Payroll and benefits information | As appropriate and agreed by the Authority, see Annex E2 | Within 5 Working Days following the Service Transfer Date | - | Authority, any Replacement Supplier and/or Replacement Sub-contractor |
| Sch 24, Annex E1 | List of Notified Sub-contractors | As appropriate and agreed by the Authority | Effective Date | Upon any change | Authority |
| Section 11 of the Front Sheet | Key Personnel | Section 11 of the Front Sheet | Effective Date | As amended from time to time | Authority |
| [If using Annex A Sch 31 - Joint Controller Agreement] Sch 26, Annex 1 Para 2.1 | Reports on Data Subject Access Requests and other Personal Data related matters | As appropriate and agreed by the Authority | As agreed with Authority | As agreed with Authority | Authority and Supplier |
| Sch 27, Annex 1 | IPR | Annex 1 to Sch 27 (Intellectual Property Rights) | As agreed with Authority | Regularly - As agreed with Authority | Authority |

Schedule 21

Exit Management

# Schedule 21: Exit Management

*[Guidance: This guidance note is for Authorities that are wider public sector bodies and are not a Central Government Body. The Ethical Wall Agreement set out in Annex 2 has been designed for use by Central Government Bodies. Any Authorities that are not Central Government Bodies will need to review and update the Authority details section, the definitions and Clause 5 (Assignment and Novation) of the Draft Ethical Wall Agreement in Annex 2 to reflect their own particular status as a wider public sector body]*

1. Definitions
   1. In this Schedule, the following definitions shall apply:

|  |  |
| --- | --- |
| “Emergency Exit” | any termination of this Contract which is a:   1. termination of the whole or part of this Contract in accordance with Clause 31 (*Termination Rights*), except where the period of notice given under that Clause is greater than or equal to 6 months; 2. termination of the provision of the Services for any reason prior to the expiry of any period of notice of termination served pursuant to Clause 31 (*Termination Rights*); or 3. wrongful termination or repudiation of this Contract by either Party; |
| “Ethical Wall Agreement” | an ethical wall agreement in a form similar to the draft ethical wall agreement set out at Annex 2; |
| “Exclusive Assets” | those Assets used by the Supplier or a Key Sub-contractor which are used exclusively in the provision of the Services; |
| “Exit Information” | has the meaning given in Paragraph 3.1; |
| “Exit Manager” | the person appointed by each Party pursuant to Paragraph 2.3 for managing the Parties’ respective obligations under this Schedule; |
| “Net Book Value” | the net book value of the relevant Asset(s) calculated in accordance with the depreciation policy of the Supplier set out in the letter in the agreed form from the Supplier to the Authority of the same date as this Contract; |
| “Non-Exclusive Assets” | those Assets (if any) which are used by the Supplier or a Key Sub-contractor in connection with the Services but which are also used by the Supplier or Key Sub-contractor for other purposes of material value; |
| “Ordinary Exit” | any termination of the whole or any part of this Contract which occurs:   1. pursuant to Clause 31 (*Termination Rights*) where the period of notice given by the Party serving notice to terminate pursuant to such Clause is greater than or equal to 6 months; or 2. as a result of the expiry of the Initial Term or any Extension Period; |
| “Transferable Assets” | those of the Exclusive Assets which are capable of legal transfer to the Authority; |
| “Transferable Contracts” | the Sub-contracts, licences for Supplier’s Software, licences for Third Party Software or other agreements which are necessary to enable the Authority or any Replacement Supplier to perform the Services or the Replacement Services, including in relation to licences all relevant Documentation; and |
| “Transferring Contracts | has the meaning given in Paragraph 7.2.3. |

1. Obligations During the Term to Facilitate Exit
   1. During the Term, the Supplier shall:
      1. create and maintain a register of all:
         1. Assets, detailing their:
         2. make, model and asset number;
         3. ownership and status as either Exclusive Assets or Non-Exclusive Assets;
         4. Net Book Value;
         5. condition and physical location; and
         6. use (including technical specifications); and
         7. Sub-contracts and other relevant agreements (including relevant software licences, maintenance and support agreements and equipment rental and lease agreements) required for the performance of the Services;
      2. create and maintain a configuration database detailing the technical infrastructure and operating procedures through which the Supplier provides the Services, which shall contain sufficient detail to permit the Authority and/or Replacement Supplier to understand how the Supplier provides the Services and to enable the smooth transition of the Services with the minimum of disruption;
      3. agree the format of the Registers with the Authority as part of the process of agreeing the Exit Plan; and
      4. at all times keep the Registers up to date, in particular in the event that Assets, Sub-contracts or other relevant agreements are added to or removed from the Services.
   2. The Supplier shall procure that all Exclusive Assets listed in the Registers are clearly marked to identify that they are exclusively used for the provision of the Services under this Contract.
   3. Each Party shall appoint a person for the purposes of managing the Parties’ respective obligations under this Schedule and provide written notification of such appointment to the other Party within 3 months of the Effective Date. The Supplier’s Exit Manager shall be responsible for ensuring that the Supplier and its employees, agents and Sub-contractors comply with this Schedule. The Supplier shall ensure that its Exit Manager has the requisite authority to arrange and procure any resources of the Supplier as are reasonably necessary to enable the Supplier to comply with the requirements set out in this Schedule. The Parties’ Exit Managers will liaise with one another in relation to all issues relevant to the termination of this Contract and all matters connected with this Schedule and each Party’s compliance with it.
2. Obligations to Assist on Re-tendering of Services
   1. On reasonable notice at any point during the Term, the Supplier shall provide to the Authority and/or its potential Replacement Suppliers (subject to the potential Replacement Suppliers entering into reasonable written confidentiality undertakings), the following material and information in order to facilitate the preparation by the Authority of any tender notice or associated tender documents and/or to facilitate any potential Replacement Suppliers undertaking due diligence:
      1. details of the Service(s);
      2. a copy of the Registers, updated by the Supplier up to the date of delivery of such Registers;
      3. an inventory of Government Data in the Supplier’s possession or control;
      4. details of any key terms of any third party contracts and licences, particularly as regards charges, termination, assignment and novation;
      5. a list of on-going and/or threatened disputes in relation to the provision of the Services;
      6. to the extent permitted by applicable Law, all information relating to Transferring Supplier Employees required to be provided by the Supplier under this Contract, and to include without limitation such information as is required to be provided under Schedule 24 (*Staff Transfer*); and
      7. such other material and information as the Authority shall reasonably require,

(together, the “Exit Information”).

* 1. The Supplier acknowledges that the Authority may disclose the Supplier’s Confidential Information to an actual or prospective Replacement Supplier or any third party whom the Authority is considering engaging to the extent that such disclosure is necessary in connection with such engagement (except that the Authority may not under this Paragraph 3.2 disclose any Supplier’s Confidential Information which is information relating to the Supplier’s or its Sub-contractors’ prices or costs).
  2. The Supplier shall:
     1. notify the Authority within 5 Working Days of any material change to the Exit Information which may adversely impact upon the potential transfer and/or continuance of any Services and shall consult with the Authority regarding such proposed material changes; and
     2. provide complete updates of the Exit Information on an as-requested basis as soon as reasonably practicable and in any event within 10 Working Days of a request in writing from the Authority or within such other time limits as may be specified within this Contract.
  3. The Supplier may charge the Authority for its reasonable additional costs to the extent the Authority requests more than 4 updates in any 6 month period.
  4. The Exit Information shall be accurate and complete in all material respects and the level of detail to be provided by the Supplier shall be such as would be reasonably necessary to enable a third party to:
     1. prepare an informed offer for those Services; and
     2. not be disadvantaged in any subsequent procurement process compared to the Supplier (if the Supplier is invited to participate).

1. Obligation to enter into an Ethical Wall Agreement on Re-tendering of Services
   1. The Authority may require the Supplier to enter into the Ethical Wall Agreement at any point during a re-tendering or contemplated re-tendering of the Services or any part of the Services.
   2. If required to enter into the Ethical Wall Agreement, the Supplier will return a signed copy of the Ethical Wall Agreement within 10 Working Days of receipt. The Supplier’s costs of entering into the Ethical Wall Agreement will be borne solely by the Supplier.
2. Exit Plan
   1. The Supplier shall, within 3 months after the Effective Date, deliver to the Authority an Exit Plan which:
      1. sets out the Supplier’s proposed methodology for achieving an orderly transition of the relevant Services from the Supplier to the Authority and/or its Replacement Supplier on the Partial Termination, expiry or termination of this Contract;
      2. complies with the requirements set out in Paragraph 5.2; and
      3. is otherwise reasonably satisfactory to the Authority.
   2. The Parties shall use reasonable endeavours to agree the contents of the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan within 20 Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.
   3. The Exit Plan shall set out, as a minimum:
      1. how the Exit Information is obtained;
      2. separate mechanisms for dealing with Ordinary Exit and Emergency Exit, the provisions relating to Emergency Exit being prepared on the assumption that the Supplier may be unable to provide the full level of assistance which is required by the provisions relating to Ordinary Exit, and in the case of Emergency Exit, provision for the supply by the Supplier of all such reasonable assistance as the Authority shall require to enable the Authority or its sub-contractors to provide the Services;
      3. a mechanism for dealing with Partial Termination on the assumption that the Supplier will continue to provide the remaining Services under this Contract;
      4. the management structure to be employed during both transfer and cessation of the Services in an Ordinary Exit and an Emergency Exit;
      5. the management structure to be employed during the Termination Assistance Period;
      6. a detailed description of both the transfer and cessation processes, including a timetable, applicable in the case of an Ordinary Exit and an Emergency Exit;
      7. how the Services will transfer to the Replacement Supplier and/or the Authority, including details of the processes, documentation, data transfer, systems migration, security and the segregation of the Authority’s technology components from any technology components operated by the Supplier or its Sub-contractors (where applicable);
      8. the scope of the Termination Services that may be required for the benefit of the Authority (including such of the services set out in Annex 1 as are applicable);
      9. a timetable and critical issues for providing the Termination Services;
      10. any charges that would be payable for the provision of the Termination Services (calculated in accordance with the methodology that would apply if such Services were being treated as a Contract Change), together with a capped estimate of such charges;
      11. how the Termination Services would be provided (if required) during the Termination Assistance Period;
      12. procedures to deal with requests made by the Authority and/or a Replacement Supplier for Staffing Information pursuant to Schedule 24 (*Staff Transfer*); and
      13. how each of the issues set out in this Schedule will be addressed to facilitate the transition of the Services from the Supplier to the Replacement Supplier and/or the Authority with the aim of ensuring that there is no disruption to or degradation of the Services during the Termination Assistance Period.
   4. The Parties acknowledge that the migration of the Services from the Supplier to the Authority and/or its Replacement Supplier may be phased, such that certain of the Services are handed over before others.
   5. The Supplier shall review and (if appropriate) update the Exit Plan on a basis consistent with the principles set out in this Schedule in the first month of each Contract Year (commencing with the second Contract Year) and if requested by the Authority following the occurrence of a Financial Distress Event, within 14 days of such request, to reflect any changes in the Services that have occurred since the Exit Plan was last agreed. Following such update, the Supplier shall submit the revised Exit Plan to the Authority for review. Within 20 Working Days following submission of the revised Exit Plan, the Parties shall meet and use reasonable endeavours to agree the contents of the revised Exit Plan. If the Parties are unable to agree the contents of the revised Exit Plan within that 20 Working Day period, such dispute shall be resolved in accordance with the Dispute Resolution Procedure.

Finalisation of the Exit Plan

* 1. Within 20 Working Days after service of a Termination Notice by either Party or 6 months prior to the expiry of this Contract, the Supplier will submit for the Authority’s approval the Exit Plan in a final form that could be implemented immediately. The final form of the Exit Plan shall be prepared on a basis consistent with the principles set out in this Schedule and shall reflect any changes in the Services that have occurred since the Exit Plan was last agreed.
  2. The Parties will meet and use their respective reasonable endeavours to agree the contents of the final form of the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan within 20 Working Days following its delivery to the Authority then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure. Until the agreement of the final form of the Exit Plan, the Supplier shall provide the Termination Services in accordance with the principles set out in this Schedule and the last approved version of the Exit Plan (insofar as relevant).

1. Termination Services

Notification of Requirements for Termination Services

* 1. The Authority shall be entitled to require the provision of Termination Services at any time during the Term by giving written notice to the Supplier (a “Termination Assistance Notice”) at least 4 months prior to the date of termination or expiry of this Contract or as soon as reasonably practicable (but in any event, not later than 1 month) following the service by either Party of a Termination Notice. The Termination Assistance Notice shall specify:
     1. the date from which Termination Services are required;
     2. the nature of the Termination Services required; and
     3. the period during which it is anticipated that Termination Services will be required, which shall continue no longer than 24 months after the expiry of the Initial Term or any Extension Period or earlier termination of this Contract;
  2. The Authority shall have:
     1. an option to extend the period of assistance beyond the period specified in the Termination Assistance Notice provided that such extension shall not extend the Termination Assistance period beyond the date which is 30 months after expiry of the Initial Term or any Extension Period or earlier termination of this Contract ;and provided that it shall notify the Supplier to such effect no later than 20 Working Days prior to the date on which the provision of Termination Services is otherwise due to expire; and
     2. the right to terminate its requirement for Termination Services by serving not less than 20 Working Days’ written notice upon the Supplier to such effect.

Termination Assistance Period

* 1. Throughout the Termination Assistance Period, or such shorter period as the Authority may require, the Supplier shall:
     1. continue to provide the Services (as applicable) and, if required by the Authority pursuant to Paragraph 6.1, provide the Termination Services;
     2. in addition to providing the Services and the Termination Services, provide to the Authority any reasonable assistance requested by the Authority to allow the Services to continue without interruption following the Partial Termination, termination or expiry of this Contract and to facilitate the orderly transfer of responsibility for and conduct of the Services to the Authority and/or its Replacement Supplier;
     3. use all reasonable endeavours to reallocate resources to provide such assistance as is referred to in Paragraph 6.3.2 without additional costs to the Authority;
     4. provide the Services and the Termination Services at no detriment to the Target Performance Levels, save to the extent that the Parties agree otherwise in accordance with Paragraph 6.5; and
     5. at the Authority’s request and on reasonable notice, deliver up-to-date Registers to the Authority.
  2. Without prejudice to the Supplier’s obligations under Paragraph 6.3.3, if it is not possible for the Supplier to reallocate resources to provide such assistance as is referred to in Paragraph 6.3.2 without additional costs to the Authority, any additional costs incurred by the Supplier in providing such reasonable assistance which is not already in the scope of the Termination Services or the Exit Plan shall be subject to the Change Control Procedure.
  3. If the Supplier demonstrates to the Authority’s reasonable satisfaction that transition of the Services and provision of the Termination Services during the Termination Assistance Period will have a material, unavoidable adverse effect on the Supplier’s ability to meet one or more particular Target Performance Level(s), the Parties shall vary the relevant Target Performance Level(s) and/or the applicable Service Credits to take account of such adverse effect.

Termination Obligations

* 1. The Supplier shall comply with all of its obligations contained in the Exit Plan in respect of any Partial Termination or termination.
  2. Upon termination or expiry (as the case may be) or at the end of the Termination Assistance Period (or earlier if this does not adversely affect the Supplier’s performance of the Services and the Termination Services and its compliance with the other provisions of this Schedule) in respect of the Services that have been terminated, the Supplier shall:
     1. cease to use the Government Data save for any Government Data that (i) the Supplier is required to retain copies of by Law (ii) is Personal Data in respect of which the Supplier is a Controller or (iii) the Supplier has rights to hold independently of this Contract;
     2. provide the Authority and/or the Replacement Supplier with a complete and uncorrupted version of the Government Data in electronic form (or such other format as reasonably required by the Authority);
     3. erase from any computers, storage devices and storage media that are to be retained by the Supplier after the end of the Termination Assistance Period all Government Data, save for any Government Data that (i) the Supplier is required to retain copies of by Law (ii) is Personal Data in respect of which the Supplier is a Controller or (iii) the Supplier has rights to hold independently of this Contract, and the Supplier shall promptly certify to the Authority that it has completed such deletion;
     4. return to the Authority such of the following as is in the Supplier’s possession or control:
        1. any parts of the IT Environment and any other equipment which belongs to the Authority; and
        2. any items that have been on-charged to the Authority, such as consumables;
     5. vacate any Authority Premises unless access is required to continue to deliver the Services;
     6. provide access during normal working hours to the Authority and/or the Replacement Supplier for up to 12 months after the Partial Termination, expiry or termination of this Contract to:
        1. such information relating to the Services as remains in the possession or control of the Supplier; and
        2. such members of the Supplier Personnel as have been involved in the design, development and provision of the Services and who are still employed by the Supplier, provided that the Authority and/or the Replacement Supplier shall pay the reasonable costs of the Supplier actually incurred in responding to requests for access under this Paragraph 6.7.6(b).
  3. Upon Partial Termination, termination or expiry (as the case may be) or at the end of the Termination Assistance Period (or earlier if this does not adversely affect the Supplier’s performance of the Services and the Termination Services and its compliance with the other provisions of this Schedule), each Party shall return to the other Party (or if requested, destroy or delete) all Confidential Information of the other Party in respect of the terminated Services and shall certify that it does not retain the other Party’s Confidential Information save to the extent (and for the limited period) that such information needs to be retained by the Party in question for the purposes of providing or receiving any Services or Termination Services or for statutory compliance purposes.

1. Assets, Sub-contracts and Software
   1. Following notice of termination or Partial Termination of this Contract and during the Termination Assistance Period, the Supplier shall not, in respect of the terminated Services, without the Authority’s prior written consent:
      1. terminate, enter into or vary any Sub-contract except to the extent that such change does not or will not affect the provision of Services or the Charges;
      2. (subject to normal maintenance requirements) make material modifications to, or dispose of, any existing Assets or acquire any new Assets; or
      3. terminate, enter into or vary any licence for Software in connection with the Services.
   2. Within 20 Working Days of receipt of the up-to-date Registers provided by the Supplier pursuant to Paragraph 6.3.5, the Authority shall provide written notice to the Supplier setting out:
      1. which, if any, of the Transferable Assets the Authority requires to be transferred to the Authority and/or the Replacement Supplier in respect of the terminated Services (“Transferring Assets”);
      2. which, if any, of:
         1. the Exclusive Assets that are not Transferable Assets; and
         2. the Non-Exclusive Assets,

the Authority and/or the Replacement Supplier requires the continued use of; and

* + 1. which, if any, of Transferable Contracts the Authority requires to be assigned or novated to the Authority and/or the Replacement Supplier (the “Transferring Contracts”),

in order for the Authority and/or its Replacement Supplier to provide the Services from the expiry of the Termination Assistance Period. Where requested by the Authority and/or its Replacement Supplier, the Supplier shall provide all reasonable assistance to the Authority and/or its Replacement Supplier to enable it to determine which Transferable Assets and Transferable Contracts the Authority and/or its Replacement Supplier requires to provide the Services or Replacement Services. Where requested by the Supplier, the Authority and/or its Replacement Supplier shall discuss in good faith with the Supplier which Transferable Contracts are used by the Supplier in matters unconnected to the Services or Replacement Services.

* 1. With effect from the expiry of the Termination Assistance Period, the Supplier shall sell the Transferring Assets to the Authority and/or its nominated Replacement Supplier for a consideration equal to their Net Book Value, except where:
     1. a Termination Payment is payable by the Authority to the Supplier, in which case, payment for such Assets shall be included within the Termination Payment; or
     2. the cost of the Transferring Asset has been partially or fully paid for through the Charges at the time of expiry or termination of this Contract, in which case the Authority shall pay the Supplier the Net Book Value of the Transferring Asset less the amount already paid through the Charges.
  2. Risk in the Transferring Assets shall pass to the Authority or the Replacement Supplier (as appropriate) at the end of the Termination Assistance Period and title to the Transferring Assets shall pass to the Authority or the Replacement Supplier (as appropriate) on payment for the same.
  3. Where the Supplier is notified in accordance with Paragraph 7.2.3 that the Authority and/or the Replacement Supplier requires continued use of any Exclusive Assets that are not Transferable Assets or any Non-Exclusive Assets, the Supplier shall as soon as reasonably practicable:
     1. procure a non-exclusive, perpetual, royalty-free licence (or licence on such other terms that have been agreed by the Authority) for the Authority and/or the Replacement Supplier to use such assets (with a right of sub-licence or assignment on the same terms); or failing which
     2. procure a suitable alternative to such assets and the Authority or the Replacement Supplier shall bear the reasonable proven costs of procuring the same.
  4. The Supplier shall as soon as reasonably practicable assign or procure the novation to the Authority and/or the Replacement Supplier of the Transferring Contracts. The Supplier shall execute such documents and provide such other assistance as the Authority reasonably requires to effect this novation or assignment.
  5. The Authority shall:
     1. accept assignments from the Supplier or join with the Supplier in procuring a novation of each Transferring Contract; and
     2. once a Transferring Contract is novated or assigned to the Authority and/or the Replacement Supplier, carry out, perform and discharge all the obligations and liabilities created by or arising under that Transferring Contract and exercise its rights arising under that Transferring Contract, or as applicable, procure that the Replacement Supplier does the same.
  6. The Supplier shall hold any Transferring Contracts on trust for the Authority until such time as the transfer of the relevant Transferring Contract to the Authority and/or the Replacement Supplier has been effected.
  7. The Supplier shall indemnify the Authority (and/or the Replacement Supplier, as applicable) against each loss, liability and cost arising out of any claims made by a counterparty to a Transferring Contract which is assigned or novated to the Authority (and/or Replacement Supplier) pursuant to Paragraph 7.6 both:
     1. in relation to any matters arising prior to the date of assignment or novation of such Sub-contract; and
     2. in relation to any matters arising after the date of assignment or novation of such Sub-contract where the loss, liability or cost arises as a result of the Supplier’s failure to comply with Clause 16 (*Intellectual Property Rights*) and/or Schedule 27 *(Intellectual Property Rights*).

1. Supplier Personnel
   1. The Authority and Supplier agree and acknowledge that in the event of the Supplier ceasing to provide the Services or part of them for any reason, Schedule 24 (*Staff Transfer*) shall apply.
   2. The Supplier shall not take any step (expressly or implicitly or directly or indirectly by itself or through any other person) to dissuade or discourage any employees engaged in the provision of the Services from transferring their employment to the Authority and/or the Replacement Supplier.
   3. During the Termination Assistance Period, the Supplier shall give the Authority and/or the Replacement Supplier reasonable access to the Supplier’s personnel to present the case for transferring their employment to the Authority and/or the Replacement Supplier.
   4. The Supplier shall immediately notify the Authority or, at the direction of the Authority, the Replacement Supplier of any period of notice given by the Supplier on disciplinary grounds in accordance with Paragraph 1.5.6 of Part E of Schedule 24 (Staff Transfer) or received from any person referred to in the Provisional Supplier Personnel List, regardless of when such notice takes effect.
   5. The Supplier shall not for a period of 12 months from the date of transfer re-employ or re-engage or entice any employees, suppliers or Sub-contractors whose employment or engagement is transferred to the Authority and/or the Replacement Supplier, except that this Paragraph shall not apply where the employee, supplier or Sub-contractor applies in response to a public advertisement of a vacancy.
2. Charges
   1. During the Termination Assistance Period (or for such shorter period as the Authority may require the Supplier to provide the Termination Services), the Authority shall pay the Charges to the Supplier in respect of the Termination Services in accordance with the rates set out in the Exit Plan (but shall not be required to pay costs in excess of the estimate set out in the Exit Plan). If the scope or timing of the Termination Services is changed and this results in a change to the costs of such Termination Services, the estimate may be varied in accordance with the Change Control Procedure.
   2. Where the Authority requests an extension to the Termination Services beyond the Termination Assistance Period in accordance with Paragraph 6.2:
      1. where more than 6 months’ notice is provided, the same rate as set out in the Exit Plan (or the Charges when not stated in the Exit Plan) shall be payable; and
      2. where less than 6 months’ notice is provided, no more than [1.2] times the rate as set out in the Exit Plan (or the Charges when not stated in the Exit Plan) shall be payable.
   3. For the purpose of calculating the costs of providing the Termination Services for inclusion in the Exit Plan or, if no Exit Plan has been agreed, the costs of providing Termination Services shall be determined in accordance with the Change Control Procedure.
   4. Except as otherwise expressly specified in this Contract, the Supplier shall not make any charges for the services provided by the Supplier pursuant to, and the Authority shall not be obliged to pay for costs incurred by the Supplier in relation to its compliance with, this Schedule including the preparation and implementation of the Exit Plan and any activities mutually agreed between the Parties to carry on after the expiry of the Termination Assistance Period.
3. Apportionments
   1. All outgoings and expenses (including any remuneration due) and all rents, royalties and other periodical payments receivable in respect of the Transferring Assets and Transferring Contracts shall be apportioned between the Authority and the Supplier and/or the Replacement Supplier and the Supplier (as applicable) as follows:
      1. the amounts shall be annualised and divided by 365 to reach a daily rate;
      2. the Authority shall be responsible for (or shall procure that the Replacement Supplier shall be responsible for) or entitled to (as the case may be) that part of the value of the invoice pro rata to the number of complete days following the transfer, multiplied by the daily rate; and
      3. the Supplier shall be responsible for or entitled to (as the case may be) the rest of the invoice.
   2. Each Party shall pay (and/or the Authority shall procure that the Replacement Supplier shall pay) any monies due under Paragraph 10.1 as soon as reasonably practicable.

## Annex 1: Scope of the Termination Services

1. Scope of the Termination Services
   1. The Termination Services to be provided by the Supplier shall include such of the following services as the Authority may specify:
      1. ceasing all non-critical Software changes (except where agreed in writing with the Authority);
      2. notifying the Sub-contractors of procedures to be followed during the Termination Assistance Period and providing management to ensure these procedures are followed;
      3. providing assistance and expertise as necessary to examine all operational and business processes (including all supporting documentation) in place and re-writing and implementing processes and procedures such that they are appropriate for use by the Authority and/or the Replacement Supplier after the end of the Termination Assistance Period;
      4. delivering to the Authority the existing systems support profiles, monitoring or system logs, problem tracking/resolution documentation and status reports all relating to the 12 month period immediately prior to the commencement of the Termination Services;
      5. providing details of work volumes and staffing requirements over the 12 month period immediately prior to the commencement of the Termination Services;
      6. with respect to work in progress as at the end of the Termination Assistance Period, documenting the current status and stabilising for continuity during transition;
      7. providing the Authority with any problem logs which have not previously been provided to the Authority;
      8. providing assistance and expertise as necessary to examine all governance and reports in place for the provision of the Services and re-writing and implementing these during and for a period of 12 months after the Termination Assistance Period;
      9. providing assistance and expertise as necessary to examine all relevant roles and responsibilities in place for the provision of the Services and re-writing and implementing these such that they are appropriate for the continuation of the Services after the Termination Assistance Period;
      10. agreeing with the Authority an effective communication strategy and joint communications plan which sets out the implications for Supplier Personnel, Authority staff, customers and key stakeholders;
      11. reviewing all Software libraries used in connection with the Services and providing details of these to the Authority and/or the Replacement Supplier;
      12. providing assistance and expertise as necessary to support the Authority and/or the Replacement Supplier develop the migration plan for business operations and Government Data to the Replacement Supplier, which may include migration approach, testing of plans, contingency options, and handling of historic or archived Government Data;
      13. provide all necessary support, equipment, tools, and Software such as data migration services and/or Automated Programming Interfaces, in order to enable and support the execution of the migration plan by the Authority and/or Replacement Supplier;
      14. making available to the Authority and/or the Replacement Supplier expertise to analyse training requirements and provide all necessary training for the use of tools by such staff as are nominated by the Authority (acting reasonably) at the time of termination or expiry;
      15. assisting in establishing naming conventions for any new production site;
      16. analysing and providing information about capacity and performance requirements, processor requirements and bandwidth requirements, and known planned requirements for capacity growth across these areas;
      17. generating a computer listing of the Source Code of **[insert** details of relevant Software] in a form and on media reasonably requested by the Authority;
      18. agreeing with the Authority a handover plan for all of the Supplier’s responsibilities as set out in the Security Management Plan;
      19. delivering copies of the production databases (with content listings) to the Authority’s and/or the Replacement Supplier’s operations staff (on appropriate media) as reasonably requested by the Authority;
      20. assisting with the loading, testing and implementation of the production databases;
      21. assisting in the execution of a parallel operation until the effective date of expiry or termination of this Contract;
      22. in respect of the maintenance and support of the Supplier System, providing historical performance data for the previous **[insert** time period];
      23. assisting in the execution of a parallel operation of the maintenance and support of the Supplier System until the end of the Termination Assistance Period or as otherwise specified by the Authority (provided that these Services shall end on a date no later than the end of the Termination Assistance Period);
      24. providing an information pack listing and describing the Services for use by the Authority in the procurement of the Replacement Services;
      25. answering all reasonable questions from the Authority and/or the Replacement Supplier regarding the Services;
      26. agreeing with the Authority and/or the Replacement Supplier a plan for the migration of the Government Data to the Authority and/or the Replacement Supplier;
      27. providing access to the Authority and/or the Replacement Supplier during the Termination Assistance Period and for a period not exceeding 6 months afterwards for the purpose of the smooth transfer of the Services to the Authority and/or the Replacement Supplier:
          1. to information and documentation relating to the Transferring Services that is in the possession or control of the Supplier or its Sub-contractors (and the Supplier agrees and shall procure that its Sub-contractors do not destroy or dispose of that information within this period) including the right to take reasonable copies of that material; and
          2. following reasonable notice and during the Supplier’s normal business hours, to members of the Supplier Personnel who have been involved in the provision or management of the Services and who are still employed or engaged by the Supplier or its Sub-contractors; and
      28. knowledge transfer services, including:
          1. transferring all training material and providing appropriate training to those Authority and/or Replacement Supplier staff responsible for internal training in connection with the provision of the Services;
          2. providing for transfer to the Authority and/or the Replacement Supplier of all knowledge reasonably required for the provision of the Services which may, as appropriate, include information, records and documents;
          3. providing the Supplier and/or the Replacement Supplier with access to such members of the Supplier’s or its Sub-contractors’ personnel as have been involved in the design, development, provision or management of the Services and who are still employed or engaged by the Supplier or its Sub-contractors; and
          4. allowing the Authority and/or the Replacement Supplier to work alongside and observe the performance of the Services by the Supplier at its Sites used to fulfil the Services (subject to compliance by the Authority and the Replacement Supplier with any applicable security and/or health and safety restrictions,

and any such person who is provided with such knowledge transfer services will sign a confidentiality undertaking in favour of the Supplier (in such form as the Supplier shall reasonably require)).

* 1. The Supplier shall:
     1. provide a documented plan relating to the training matters referred to in Paragraph 1.1.14 for agreement by the Authority at the time of termination or expiry of this Contract;
     2. co-operate fully in the execution of the handover plan agreed pursuant to Paragraph 1.1.18, providing skills and expertise of a suitable standard; and
     3. fully co-operate in the execution of the Government Data migration plan agreed pursuant to Paragraph 1.1.26, providing skills and expertise of a reasonably acceptable standard.
  2. To facilitate the transfer of knowledge from the Supplier to the Authority and/or its Replacement Supplier, the Supplier shall provide a detailed explanation of the procedures and operations used to provide the Services, the change management process and other standards and procedures to the operations personnel of the Authority and/or the Replacement Supplier.
  3. The information which the Supplier shall provide to the Authority and/or the Replacement Supplier pursuant to Paragraph 1.1.27 shall include:
     1. copies of up-to-date procedures and operations manuals;
     2. product information;
     3. agreements with third party suppliers of goods and services which are to be transferred to the Authority and/or the Replacement Supplier;
     4. key support contact details for third party supplier personnel under contracts which are to be assigned or novated to the Authority pursuant to this Schedule;
     5. information regarding any unresolved faults in progress at the commencement of the Termination Assistance Period as well as those expected to be in progress at the end of the Termination Assistance Period;
     6. details of physical and logical security processes and tools which will be available to the Authority; and
     7. any relevant interface information,

and such information shall be updated by the Supplier at the end of the Termination Assistance Period.

* 1. During the Termination Assistance Period the Supplier shall grant any agent or personnel (including employees, consultants and Suppliers) of the Replacement Supplier and/or the Authority access, during business hours and upon reasonable prior written notice, to any Sites for the purpose of effecting a prompt knowledge transfer provided that:
     1. any such agent or personnel (including employees, consultants and suppliers) having access to any Sites pursuant to this Paragraph 1.5 shall:
        1. sign a confidentiality undertaking in favour of the Supplier (in such form as the Supplier shall reasonably require); and
        2. during each period of access comply with the security, systems and facilities operating procedures of the Supplier relevant to such Site and that the Authority deems reasonable; and
     2. the Authority and/or the Replacement Supplier shall pay the reasonable, proven and proper costs of the Supplier incurred in facilitating such access.

## Annex 2: Draft Ethical Wall Agreement

[THE AUTHORITY]

and

[THE COUNTERPARTY]

ETHICAL WALL AGREEMENT

This Agreement is dated [ ] 20[ ] (the “Effective Date”).

BETWEEN:

1. **[insert NAME OF AUTHORITY]** (the “**Authority**”) [acting on behalf of the Crown] of **[insert** Authority’s address]; and
2. **[NAME OF COUNTERPARTY]** a [company]/[limited liability partnership] registered in England and Wales under registered number **[insert** registered number] whose registered office is at **[insert** Counterparty’s registered address] (the “**Counterparty**”),

together the “**Parties**” and each a “**Party**”.

BACKGROUND

(A) The Authority in relation to its procurement process must treat suppliers the same unless a difference between the suppliers justifies different treatment, pursuant to the Procurement Act 2023 and any regulations made under it. The purpose of this document (**"Agreement"**) is to define the protocols to be followed to prevent, identify and remedy any conflict of interest (whether actual, potential or perceived) in the context of the Purpose (defined below).

(B) The Authority is conducting a procurement exercise for the [supply/purchase/provision] of **[insert** details of project/goods/services] (the “**Purpose**”).

(C) The Parties wish to enter into this Agreement to ensure that a set of management processes, barriers and disciplines are put in place to ensure that conflicts of interest do not arise, and that the Counterparty does not obtain an unfair competitive advantage over Other Bidders.

IT IS AGREED:

1. Definitions and Interpretation
   1. The following capitalised words and expressions shall have the following meanings in this Agreement and its recitals:

“**Affiliate**” means in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control of that body corporate from time to time;

“**Agreement**” means this ethical walls agreement duly executed by the Parties;

“**Bid Team**” means any Representatives of the Counterparty, any of its Affiliates and/or any Subcontractors connected to the preparation of a Tender Response;

“**Central Government Body**” means a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics, including:

* + - 1. Government Departments;
      2. Non-Departmental Public Bodies or Assembly Sponsored Public Bodies (advisory, executive, or tribunal);
      3. Non-Ministerial Departments; or
      4. Executive Agencies;

“**Conflicted Personnel**” means any Representatives of:

* + - 1. the Counterparty;
      2. any of the Counterparty’s Affiliates; and/or
      3. any Subcontractors,

who, because of the Counterparty’s, any of its Affiliates’ and/or any Subcontractors’ relationship with the Authority under any Contract, have or have had access to information which creates or may create a conflict of interest or provide the Bid Team with an unfair advantage as regards information Other Bidders would not have;

“**Contract**” means any pre-existing or previous contract between the Authority and:

* + - 1. the Counterparty;
      2. any of the Counterparty’s Affiliates;
      3. any Subcontractor; and
      4. any other Third Party,

relating to the subject matter of the Purpose at the date of the commencement of the Tender Process;

“**Control**” means the beneficial ownership of more than 50% of the issued share capital of a company or the legal power to direct or cause the direction of the management of the company and “**Controls**” and “**Controlled**” shall be interpreted accordingly;

“**Effective Date**” means the date of this Agreement as set out above;

“**Other Bidder**”means any other bidder or potential bidder that is not the Counterparty or any of its Affiliates that has taken or is taking part in the Tender Process;

“**Procurement Process**” means the period commencing on the earlier of: (a) the publication of the first notice in relation to the Purpose; and (b) the execution of this Agreement, and ending on the occurrence of: (i) the publication by the Authority of the contract details notice that result from the Tender Process; or (ii) the abandonment or termination of the Tender Process as notified by the Authority;

“**Professional Advisor**” means a supplier, subcontractor, advisor or consultant engaged by the Counterparty and/or any of its Affiliates under the auspices of compiling its Tender Response;

“**Purpose**” has the meaning given to it in recital B to this Agreement;

“**Representative**”refers to a person’s officers, directors, employees, advisers (including the officers, directors, employees, advisers and agents of any Professional Advisors), agents and, where the context admits, providers or potential providers of finance (including their representatives) to the Counterparty, any of its Affiliates and/or any subcontractors engaged in connection with the Tender Process;

“**Subcontractor**” means an existing or proposed subcontractor of:

* + - 1. the Counterparty; and/or
      2. any of the Counterparty’s Affiliates,

who is connected to the preparation of a Tender Response (including key subcontractors named in the Tender Response);

"**Tender Process**"means, with regard to the Purpose, the relevant procedure provided for in the Procurement Act 2023 and any regulations made under it, which the Authority has elected to use to select a contractor or contractors, together with all relevant information, data, correspondence and/or documents issued and/or made available by or on behalf of the Authority as part of that procurement exercise and all information, correspondence and/or documents issued and/or made available by or on behalf of the bidders in response together with any resulting contracts;

"**Tender Response**" means the tender(s) submitted, or to be submitted, by the Counterparty, any of its Affiliates and/or any Subcontractors in response to any invitation(s) to submit bids under the Tender Process;

“**Third Party**” means any person who is not a Party, including Other Bidders, their Affiliates and/or their Representatives; and

“**Working Day**” means any day of the week other than a weekend, when Banks in England and Wales are open for business.

* 1. Reference to the disclosure of information includes any communication or making available information and includes both direct and indirect disclosure.
  2. Reference to the disclosure of information, or provision of access, by or to the Authority, the Counterparty, any of the Counterparty’s Affiliates and/or any Subcontractors includes disclosure, or provision of access, by or to the Representatives of the Authority, the Counterparty, any of its Affiliates and/or any Subcontractors (as the case may be).
  3. Reference to persons includes legal and natural persons.
  4. Reference to any enactment is to that enactment as amended, supplemented, re-enacted or replaced from time to time.
  5. Reference to Clauses and recitals is to clauses of and recitals to this Agreement.
  6. Reference to any gender includes any other.
  7. Reference to writing includes email.
  8. The terms “**associate**”, “**holding company**”, “**subsidiary**”, “**subsidiary undertaking**” and “**wholly owned subsidiary**” have the meanings attributed to them in the Companies Act 2006, except that for the purposes of section 1159(1)(a) of that Act, the words ‘holds a majority of the voting rights’ shall be changed to ‘holds 30% or more of the voting rights’, and other expressions shall be construed accordingly.
  9. The words “**include**” and “**including**” are to be construed without limitation.
  10. The singular includes the plural and vice versa.
  11. The headings contained in this Agreement shall not affect its construction or interpretation.

1. Ethical Walls
   1. In consideration of the sum of £1 payable by the Authority to the Counterparty, receipt of which is hereby acknowledged, the Parties agree to be bound by the terms of this Agreement.

Conflicts of Interest

* 1. The Counterparty:
     1. shall take all appropriate steps to ensure that neither the Counterparty, nor its Affiliates, nor any Subcontractors nor any Representatives are in a position where, in the reasonable opinion of the Authority, there is or may be an actual conflict, or a potential conflict, between the pecuniary or personal interests of the Counterparty, any of its Affiliates, any Subcontractors and/or any Representatives and the duties owed to the Authority under any Contract or pursuant to an open and transparent Tender Process; and
     2. acknowledges and agrees that a conflict of interest may arise in situations where the Counterparty, any of its Affiliates, any Subcontractors and/or any Representatives intend to take part in the Tender Process and because of the Counterparty’s, any of its Affiliates’, any Subcontractors’ and/or any Representatives’ relationship with the Authority under any Contract, the Counterparty, any of its Affiliates, any Subcontractors and/or any Representatives have or have had access to information which could provide the Counterparty, any of its Affiliates, any Subcontractors and/or any Representatives with an advantage and render unfair an otherwise genuine and open competitive Tender Process.
  2. Where there is or is likely to be a conflict of interest, or the perception of a conflict of interest, of any kind in relation to the Tender Process, the Counterparty shall take such steps that are necessary to eliminate the conflict of interest to the Authority’s satisfaction, including one or more of the following:
     1. not assigning any of the Conflicted Personnel to the Bid Team at any time;
     2. providing to the Authority promptly upon request a complete and up to date list of any Conflicted Personnel and the personnel comprising the Bid Team and reissue such list to the Authority promptly upon any change to it;
     3. ensuring that no act or omission by itself, its Affiliates, any Subcontractors and/or any Representatives results in information of any kind, however conveyed, or in any format and however so stored:
        1. about the Tender Process (gleaned from the performance of any Contract or otherwise); and/or
        2. which would or could in the opinion of the Authority confer an unfair advantage on the Counterparty in relation to its participation in the Tender Process,

becoming available to the Bid Team where the Authority has not made generally available that information to Other Bidders;

* + 1. ensuring that by no act or omission by itself, its Affiliates, any Subcontractors and/or any Representatives and in particular the Bid Team results in information of any kind, however conveyed, in any format and however so stored about the Tender Process, its operation and all matters connected or ancillary to it becoming available to the Conflicted Personnel;
    2. ensure that agreements that flow down the Counterparty’s obligations in this Agreement, are entered into as necessary, between the Counterparty and its Affiliates and any Subcontractors [in a form to be approved by the Authority];
    3. physically separating the Conflicted Personnel and the Bid Team, either in separate buildings or in areas with restricted access;
    4. providing regular training to its Affiliates, any Subcontractors and/or Representatives to ensure it is complying with this Agreement;
    5. monitoring Conflicted Personnel movements within restricted areas (both physical and electronic online areas) to ensure it is complying with this Agreement and to ensure adherence to the ethical wall arrangements the Counterparty, its Affiliates, any Subcontractors and/or any Representatives have put in place in order to comply with this Agreement;
    6. ensuring that the Conflicted Personnel and the Bid Team are line managed and report independently of each other; and
    7. complying with any other action as the Authority, acting reasonably, may direct in connection with the Tender Process and/or this Agreement.

Notification of Conflicts of Interest

* 1. The Counterparty shall:
     1. notify the Authority immediately in writing of all perceived, potential and/or actual conflicts of interest that arise or have arisen;
     2. submit in writing to the Authority full details of the nature of the perceived, potential and/or actual conflict of interest including full details of the risk assessments undertaken, the impact or potential impact of the perceived, potential and/or actual conflict, the measures and arrangements that have been established and/or are due to be established, to eliminate the perceived, potential and/or actual conflict, and the Counterparty’s plans to prevent potential conflicts of interests from arising (“**Proposed Avoidance Measures**”); and
     3. seek the Authority’s approval to the Proposed Avoidance Measures which the Authority shall have the right to grant, grant conditionally or deny (if the Authority rejects the Proposed Avoidance Measures the Counterparty shall repeat the process set out in this Clause 2.4 until such time as the Authority grants approval or the Counterparty withdraws from the Tender Process).
  2. The Counterparty will provide to the Authority, on demand, any and all information in relation to its adherence with its obligations set out under Clauses 2.2 and 2.3 as reasonably requested by the Authority.
  3. The Authority reserves the right to require the Counterparty to demonstrate the measures put in place by the Counterparty under Clauses 2.2 and 2.3.
  4. The Counterparty acknowledges that any provision of information or demonstration of measures, in accordance with Clauses 2.5 and 2.6, does not constitute acceptance by the Authority of the adequacy of such measures and does not discharge the Counterparty of its obligations or liability under this Agreement.

Exclusion from the Tender Process

* 1. Where, in the reasonable opinion of the Authority, there has been any breach by the Counterparty of Clauses 2.2, 2.3, or 2.4 or failure to obtain the Authority’s approval of the Proposed Avoidance Measures the Authority shall be entitled to exclude the Counterparty, or any of its Affiliates and/or any Representatives, from the Tender Process, and the Authority may, in addition to the right to exclude, take such other steps as it deems necessary.
  2. The actions of the Authority pursuant to Clause 2.8 shall not prejudice or affect any right of action or remedy under this Agreement or at law which shall have accrued or shall thereafter accrue to the Authority.

Bid Costs

* 1. In no event shall the Authority be liable for any bid costs incurred by:
     1. the Counterparty or any of its Affiliates, any Representatives and/or any Subcontractors; or
     2. any Third Party,

as a result of any breach of this Agreement by the Counterparty, any of its Affiliates, any Subcontractors and/or Representatives, including where the Counterparty, any of its Affiliates, any Subcontractors or Representatives, or any Third Party is or are excluded from the Tender Process.

Specific Remedies

* 1. The Counterparty acknowledges and agrees that:
     1. neither damages nor specific performance are adequate remedies in the event of a breach of the obligations in Clause 2; and
     2. in the event of a breach of any of the obligations in Clause 2 which cannot be effectively remedied the Authority shall have the right to terminate both this Agreement and the Counterparty’s participation in the Tender Process in each case with immediate effect on written notice.

1. Sole Responsibility
   1. It is the sole responsibility of the Counterparty to comply with the terms of this Agreement, including ensuring its Affiliates, any Subcontractors, and/or any Representatives comply with the terms of this Agreement. No approval by the Authority of any procedures, agreements or arrangements provided by the Counterparty, any of its Affiliates, any Subcontractors and/or their Representatives to the Authority shall discharge the Counterparty’s obligations.
2. Waiver and Invalidity
   1. No failure or delay by any Party in exercising any right, power or privilege under this Agreement or by law shall constitute a waiver of that or any other right, power or privilege, nor shall it restrict the further exercise of that or any other right, power or privilege. No single or partial exercise of such right, power or privilege shall prevent or restrict the further exercise of that or any other right, power or privilege.
   2. If any provision of this Agreement is prohibited or unenforceable in any jurisdiction in relation to any Party, such prohibition or unenforceability will not invalidate the remaining provisions of this Agreement, or affect the validity or enforceability of the provisions of this Agreement in relation to any other Party or any other jurisdiction.
3. Assignment and Novation
   1. The Counterparty shall not assign, novate or otherwise dispose of or create any trust in relation to any or all of its rights, obligations or liabilities under this Agreement without the prior written consent of the Authority.
   2. The Authority may assign, novate or otherwise dispose of any or all of its rights, obligations and liabilities under this Agreement and/or any associated licences to:
      1. any Central Government Body; or
      2. to a body other than a Central Government Body (including any private sector body) which performs any of the functions that previously had been performed by the Authority; and
      3. the Counterparty shall, at the Authority’s request, enter into a novation agreement in such form as the Authority may reasonably specify in order to enable the Authority to exercise its rights pursuant to this Clause 5.
   3. A change in the legal status of the Authority such that it ceases to be a Central Government Body shall not affect the validity of this Agreement and this Agreement shall be binding on any successor body to the Authority.
4. Contracts (Rights of Third Parties) Act 1999
   1. A person who is not a Party to this Agreement has no right under the Contract (Rights of Third Parties) Act 1999 (as amended, updated or replaced from time to time) to enforce any term of this Agreement, but this does not affect any right or remedy of any person which exists or is available otherwise than pursuant to that Act.
5. Transparency
   1. The Parties acknowledge and agree that the Authority is under a legal duty pursuant to the Procurement Act 2023 and any regulations made under it to run procurement processes in accordance with section 12 of the Procurement Act 2023. Accordingly, the Authority may disclose the contents of this Agreement to Other Bidders (and/or potential Other Bidders) for the purposes of transparency and in order to evidence that a fair procurement process has been followed.
6. Notices
   1. Any notices sent under this Agreement shall be in writing and be served by e-mail unless it is not practicable to do so.
   2. Subject to Clause 8.1, the following table sets out the method by which notices may be served under this Agreement and the respective deemed time and proof of service:

| Manner of Delivery | Deemed time of service | Proof of service |
| --- | --- | --- |
| E-mail. | 9.00am on the first Working Day after sending | Dispatched as a pdf attachment to an e-mail to the correct e-mail address without any error message. |
| Personal delivery. | On delivery, provided delivery is between 9.00am and 5.00pm on a Working Day. Otherwise, delivery will occur at 9.00am on the next Working Day. | Properly addressed and delivered as evidenced by signature of a delivery receipt. |
| Prepaid, Royal Mail Signed For™ 1st Class or other prepaid, next Working Day service providing proof of delivery. | At the time recorded by the delivery service, provided that delivery is between 9.00am and 5.00pm on a Working Day. Otherwise, delivery will occur at 9.00am on the same Working Day (if delivery before 9.00am) or on the next Working Day (if after 5.00pm). | Properly addressed prepaid and delivered as evidenced by signature of a delivery receipt. |

* 1. Notices shall be sent to the e-mail addresses (or address, where e-mail is not practicable) set out below or at such other address as the relevant Party may give notice to the other Party for the purpose of service of notices under this Agreement:

|  | Counterparty | Authority |
| --- | --- | --- |
| **Contact** |  |  |
| **E-mail** |  |  |
| **Address** |  |  |

* 1. This Clause 8 does not apply to the service of any proceedings or other documents in any legal action or other method of dispute resolution.

1. Waiver and Cumulative Remedies
   1. The rights and remedies under this Agreement may be waived only by notice, and in a manner that expressly states that a waiver is intended. A failure or delay by a Party in ascertaining or exercising a right or remedy provided under this Agreement or by law shall not constitute a waiver of that right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of any right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.
   2. Unless otherwise provided in this Agreement, rights and remedies under this Agreement are cumulative and do not exclude any rights or remedies provided by law, in equity or otherwise.
2. Term
   1. Each Party’s obligations under this Agreement shall continue in full force and effect for period of [ ] years from the Effective Date/[or for the period of the duration of the Procurement Process]
3. Governing Law and Jurisdiction
   1. This Agreement and any issues, disputes or claims (whether contractual or non-contractual) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the laws of England and Wales.
   2. The Parties agree that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (whether contractual or non-contractual) that arises out of or in connection with this Agreement or its subject matter or formation.

|  |  |
| --- | --- |
| Signed by the Authority | Name:  Signature:  Position in Authority: |

|  |  |
| --- | --- |
| Signed by the Counterparty | Name:  Signature:  Position in Counterparty: |

Schedule 22

Service Continuity Plan and Corporate Resolution Planning

# Schedule 22: Service Continuity Plan and Corporate Resolution Planning

## Part A: Service Continuity Plan

1. Definitions
   1. In this Schedule, the following definitions shall apply:

|  |  |
| --- | --- |
| “Business Continuity Plan” | has the meaning given in Paragraph 2.2.1(b); |
| “Business Continuity Services” | has the meaning given in Paragraph 4.2.2; |
| “Department” | a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics:   1. Government Department; or 2. Non-Ministerial Department. |
| “Disaster” | the occurrence of one or more events which, either separately or cumulatively, mean that the Services, or a material part of the Services will be unavailable for a period of [insert details] or which is reasonably anticipated will mean that the Services or a material part of the Services will be unavailable for that period; |
| “Disaster Recovery Plan” | has the meaning given in Paragraph 2.2.1(c); |
| “Disaster Recovery Services” | the services embodied in the processes and procedures for restoring the Services following the occurrence of a Disaster; |
| “Disaster Recovery System” | the system identified by the Supplier in the Supplier Solution which shall be used for the purpose of delivering the Disaster Recovery Services; |
| “Insolvency Continuity Plan” | has the meaning given in Paragraph 2.2.1(d). |
| “Related Service Provider” | any person who provides services to the Authority in relation to this Contract from time to time, which persons include as at the Effective Date [insert details]; |
| “Review Report” | has the meaning given in Paragraphs 7.2.1 to 7.2.3; and |
| “Service Continuity Plan” | means the plan prepared pursuant to Paragraph 2 of this Schedule which incorporates the Business Continuity Plan, Disaster Recovery Plan and the Insolvency Continuity Plan. |

1. Service Continuity Plan
   1. Within 40 Working Days from the Effective Date the Supplier shall prepare and deliver to the Authority for the Authority’s written approval a plan, which shall detail the processes and arrangements that the Supplier shall follow to:
      1. ensure continuity of the business processes and operations supported by the Services following any failure or disruption of any element of the Services (including where caused by an Insolvency Event of the Supplier, any Key Sub-contractor and/or any Supplier Group member); and
      2. the recovery of the Services in the event of a Disaster.
   2. The Service Continuity Plan shall:
      1. be divided into four parts:
         1. Part A which shall set out general principles applicable to the Service Continuity Plan;

* + - 1. Part B which shall relate to business continuity (the “Business Continuity Plan”);

* + - 1. Part C which shall relate to disaster recovery (the “Disaster Recovery Plan”);

* + - 1. Part D which shall relate to an Insolvency Event of the Supplier, any Key Sub-contractors and/or any Supplier Group member (the “Insolvency Continuity Plan”); and
    1. unless otherwise required by the Authority in writing, be based upon and be consistent with the provisions of Paragraphs 3, 4, 5 and 6.
  1. Following receipt of the draft Service Continuity Plan from the Supplier, the Authority shall:
     1. review and comment on the draft Service Continuity Plan as soon as reasonably practicable; and
     2. notify the Supplier in writing that it approves or rejects the draft Service Continuity Plan no later than 20 Working Days after the date on which the draft Service Continuity Plan is first delivered to the Authority.
  2. If the Authority rejects the draft Service Continuity Plan:
     1. the Authority shall inform the Supplier in writing of its reasons for its rejection; and
     2. the Supplier shall then revise the draft Service Continuity Plan (taking reasonable account of the Authority’s comments) and shall re-submit a revised draft Service Continuity Plan to the Authority for the Authority’s approval within 20 Working Days of the date of the Authority’s notice of rejection. The provisions of Paragraph 2.3 and this Paragraph 2.4 shall apply again to any resubmitted draft Service Continuity Plan, provided that either Party may refer any disputed matters for resolution by the Dispute Resolution Procedure at any time.

1. Service Continuity Plan: Part A – General Principles and Requirements
   1. Part A of the Service Continuity Plan shall:
      1. set out how the business continuity, disaster recovery and insolvency continuity elements of the plan link to each other;
      2. provide details of how the invocation of any element of the Service Continuity Plan may impact upon the operation of the Services and any services provided to the Authority by a Related Service Provider;
      3. contain an obligation upon the Supplier to liaise with the Authority and (at the Authority’s request) any Related Service Provider with respect to issues concerning business continuity, disaster recovery and insolvency continuity where applicable;
      4. detail how the Service Continuity Plan links and interoperates with any overarching and/or connected disaster recovery, business continuity and/or insolvency continuity plan of the Authority and any of its other Related Service Providers in each case as notified to the Supplier by the Authority from time to time;
      5. contain a communication strategy including details of an incident and problem management service and advice and help desk facility which can be accessed via multi-channels (including but without limitation a web-site (with FAQs), e-mail, phone and fax) for both portable and desk top configurations, where required by the Authority;
      6. contain a risk analysis, including:
         1. failure or disruption scenarios and assessments and estimates of frequency of occurrence;
         2. identification of any single points of failure within the Services and processes for managing the risks arising therefrom;
         3. identification of risks arising from the interaction of the Services with the services provided by a Related Service Provider;
         4. identification of risks arising from an Insolvency Event of the Supplier, any Key Sub-contractors and/or Supplier Group member; and
         5. a business impact analysis (detailing the impact on business processes and operations) of different anticipated failures or disruptions;
      7. provide for documentation of processes, including business processes, and procedures;
      8. set out key contact details (including roles and responsibilities) for the Supplier (and any Sub-contractors) and for the Authority;
      9. identify the procedures for reverting to “normal service”;
      10. the Backup and Recovery Plan prepared under Schedule 5 *(Security Management)*;
      11. identify the responsibilities (if any) that the Authority has agreed it will assume in the event of the invocation of the Service Continuity Plan; and
      12. provide for the provision of technical advice and assistance to key contacts at the Authority as notified by the Authority from time to time to inform decisions in support of the Authority’s business continuity plans.
   2. The Service Continuity Plan shall be designed so as to ensure that:
      1. the Services are provided in accordance with this Contract at all times during and after the invocation of the Service Continuity Plan;
      2. the adverse impact of any Disaster; service failure; an Insolvency Event of the Supplier, any Key Sub-contractor and/or any Supplier Group member; or disruption on the operations of the Authority, is minimal as far as reasonably possible;
      3. it complies with the relevant provisions of ISO/IEC 22301 and all other industry standards from time to time in force; and
      4. there is a process for the management of disaster recovery testing detailed in the Service Continuity Plan.
   3. The Service Continuity Plan shall be upgradeable and sufficiently flexible to support any changes to the Services, to the business processes facilitated by and the business operations supported by the Services, and/or changes to the Supplier Group structure.
   4. The Supplier shall not be entitled to any relief from its obligations under the Performance Indicators or to any increase in the Charges to the extent that a Disaster occurs as a consequence of any breach by the Supplier of this Contract.
2. Service Continuity Plan: Part B – Business Continuity

Principles and Contents

* 1. The Business Continuity Plan shall set out the arrangements that are to be invoked to ensure that the business processes and operations facilitated by the Services remain supported and to ensure continuity of the business operations supported by the Services including, unless the Authority expressly states otherwise in writing:
     1. the alternative processes (including business processes), options and responsibilities that may be adopted in the event of a failure in or disruption to the Services; and
     2. the steps to be taken by the Supplier upon resumption of the Services in order to address any prevailing effect of the failure or disruption including a root cause analysis of the failure or disruption.
  2. The Business Continuity Plan shall:
     1. address the various possible levels of failures of or disruptions to the Services;
     2. set out the services to be provided and the steps to be taken to remedy the different levels of failures of and disruption to the Services (such services and steps, the “Business Continuity Services”);
     3. specify any applicable Performance Indicators with respect to the provision of the Business Continuity Services and details of any agreed relaxation to the Performance Indicators in respect of other Services during any period of invocation of the Business Continuity Plan; and
     4. clearly set out the conditions and/or circumstances under which the Business Continuity Plan is invoked.

1. Service Continuity Plan: Part C – Disaster Recovery

Principles and Contents

* 1. The Disaster Recovery Plan shall be designed so as to ensure that upon the occurrence of a Disaster the Supplier ensures continuity of the business operations of the Authority supported by the Services following any Disaster or during any period of service failure or disruption with, as far as reasonably possible, minimal adverse impact.
  2. The Disaster Recovery Plan shall be invoked only upon the occurrence of a Disaster.
  3. The Disaster Recovery Plan shall include the following:
     1. the technical design and build specification of the Disaster Recovery System;
     2. details of the procedures and processes to be put in place by the Supplier in relation to the Disaster Recovery System and the provision of the Disaster Recovery Services and any testing of the same including but not limited to the following:
        1. data centre and disaster recovery site audits;
        2. the Backup and Recovery Plan prepared under Schedule 5 *(Security Management)*;
        3. identification of all potential disaster scenarios;
        4. risk analysis;
        5. documentation of processes and procedures;
        6. hardware configuration details;
        7. network planning including details of all relevant data networks and communication links;
        8. invocation rules;
        9. Service recovery procedures; and
        10. steps to be taken upon resumption of the Services to address any prevailing effect of the failure or disruption of the Services;
     3. any applicable Performance Indicators with respect to the provision of the Disaster Recovery Services and details of any agreed relaxation to the Performance Indicators in respect of other Services during any period of invocation of the Disaster Recovery Plan;
     4. details of how the Supplier shall ensure compliance with security standards ensuring that compliance is maintained for any period during which the Disaster Recovery Plan is invoked;
     5. access controls to any disaster recovery sites used by the Supplier in relation to its obligations pursuant to this Schedule; and
     6. testing and management arrangements.

1. Service Continuity Plan: Part D – Insolvency Continuity Plan

Principles and Contents

* 1. The Insolvency Continuity Plan shall be designed by the Supplier to permit continuity of the business operations of the Authority supported by the Services through continued provision of the Services following an Insolvency Event of the Supplier, any Key Sub-contractor and/or any Supplier Group member with, as far as reasonably possible, minimal adverse impact.
  2. The Insolvency Continuity Plan shall include the following:
     1. communication strategies which are designed to minimise the potential disruption to the provision of the Services, including key contact details in respect of the supply chain and key contact details for operational and contract Supplier Personnel, Key Sub-contractor personnel and Supplier Group member personnel;
     2. identification, explanation, assessment and an impact analysis of risks in respect of dependencies between the Supplier, Key Sub-contractors and Supplier Group members where failure of those dependencies could reasonably have an adverse impact on the Services;
     3. plans to manage and mitigate identified risks;
     4. details of the roles and responsibilities of the Supplier, Key Sub-contractors and/or Supplier Group members to minimise and mitigate the effects of an Insolvency Event of such persons on the Services;
     5. details of the recovery team to be put in place by the Supplier (which may include representatives of the Supplier, Key Sub-contractors and Supplier Group members); and
     6. sufficient detail to enable an appointed insolvency practitioner to invoke the plan in the event of an Insolvency Event of the Supplier.

1. Review and Amendment of the Service Continuity Plan
   1. The Supplier shall review and update the Service Continuity Plan (and the risk analysis on which it is based):
      1. on a regular basis and as a minimum once every [6 months / 12 months];
      2. within three calendar months of the Service Continuity Plan (or any part) having been invoked pursuant to Paragraph 9;
      3. within 14 days of a Financial Distress Event;
      4. within 30 days of a Corporate Change Event (unless the Relevant Authority (acting reasonably) agrees to a Corporate Change Event Grace Period, as set out in Paragraph 2.8.2(a), in which case that Corporate Change Event Grace Period will apply); and
      5. where the Authority requests any additional reviews (over and above those provided for in Paragraphs 7.1.1 to 7.1.4) by notifying the Supplier to such effect in writing, whereupon the Supplier shall conduct such reviews in accordance with the Authority’s written requirements. Prior to starting its review, the Supplier shall provide an accurate written estimate of the total costs payable by the Authority for the Authority’s approval. The costs of both Parties of any such additional reviews shall be met by the Authority except that the Supplier shall not be entitled to charge the Authority for any costs that it may incur above any estimate without the Authority’s prior written approval.
   2. Each review of the Service Continuity Plan pursuant to Paragraph 7.1 shall be a review of the procedures and methodologies set out in the Service Continuity Plan and shall assess their suitability having regard to any change to the Services or any underlying business processes and operations facilitated by or supported by the Services which have taken place since the later of the original approval of the Service Continuity Plan or the last review of the Service Continuity Plan and shall also have regard to any occurrence of any event since that date (or the likelihood of any such event taking place in the foreseeable future) which may increase the likelihood of the need to invoke the Service Continuity Plan. The review shall be completed by the Supplier within the period required by the Service Continuity Plan or, if no such period is required, within such period as the Authority shall reasonably require. The Supplier shall, within 20 Working Days of the conclusion of each such review of the Service Continuity Plan, provide to the Authority a report (a “Review Report”) setting out:
      1. the findings of the review;
      2. any changes in the risk profile associated with the Services; and
      3. the Supplier’s proposals (the “Supplier’s Proposals”) for addressing any changes in the risk profile and its proposals for amendments to the Service Continuity Plan following the review detailing the impact (if any and to the extent that the Supplier can reasonably be expected to be aware of the same) that the implementation of such proposals may have on any services or systems provided by a third party.
   3. Following receipt of the Review Report and the Supplier’s Proposals, the Authority shall:
      1. review and comment on the Review Report and the Supplier’s Proposals as soon as reasonably practicable; and
      2. notify the Supplier in writing that it approves or rejects the Review Report and the Supplier’s Proposals no later than 20 Working Days after the date on which they are first delivered to the Authority.
   4. If the Authority rejects the Review Report and/or the Supplier’s Proposals:
      1. the Authority shall inform the Supplier in writing of its reasons for its rejection; and
      2. the Supplier shall then revise the Review Report and/or the Supplier’s Proposals as the case may be (taking reasonable account of the Authority’s comments and carrying out any necessary actions in connection with the revision) and shall re-submit a revised Review Report and/or revised Supplier’s Proposals to the Authority for the Authority’s approval within 20 Working Days of the date of the Authority’s notice of rejection. The provisions of Paragraph 7.3 and this Paragraph 7.4 shall apply again to any resubmitted Review Report and Supplier’s Proposals, provided that either Party may refer any disputed matters for resolution by the Dispute Resolution Procedure at any time.
   5. The Supplier shall as soon as is reasonably practicable after receiving the Authority’s approval of the Supplier’s Proposals (having regard to the significance of any risks highlighted in the Review Report) effect any change in its practices or procedures necessary so as to give effect to the Supplier’s Proposals. Any such change shall be at the Supplier’s expense unless it can be reasonably shown that the changes are required because of a material change to the risk profile of the Services.
2. Testing of the Service Continuity Plan
   1. The Supplier shall test the Service Continuity Plan on a regular basis (and in any event not less than once in every Contract Year). Subject to Paragraph 8.2, the Authority may require the Supplier to conduct additional tests of some or all aspects of the Service Continuity Plan at any time where the Authority considers it necessary, including where there has been any change to the Services or any underlying business processes, or on the occurrence of any event which may increase the likelihood of the need to implement the Service Continuity Plan.
   2. If the Authority requires an additional test of the Service Continuity Plan, it shall give the Supplier written notice and the Supplier shall conduct the test in accordance with the Authority’s requirements and the relevant provisions of the Service Continuity Plan. The Supplier’s costs of the additional test shall be borne by the Authority unless the Service Continuity Plan fails the additional test in which case the Supplier’s costs of that failed test shall be borne by the Supplier.
   3. The Supplier shall undertake and manage testing of the Service Continuity Plan in full consultation with the Authority and shall liaise with the Authority in respect of the planning, performance, and review, of each test, and shall comply with the reasonable requirements of the Authority in this regard. Each test shall be carried out under the supervision of the Authority or its nominee.
   4. The Supplier shall ensure that any use by it or any Sub-contractor of “live” data in such testing is first approved with the Authority. Copies of live test data used in any such testing shall be (if so required by the Authority) destroyed or returned to the Authority on completion of the test.
   5. The Supplier shall, within 20 Working Days of the conclusion of each test, provide to the Authority a report setting out:
      1. the outcome of the test;
      2. any failures in the Service Continuity Plan (including the Service Continuity Plan’s procedures) revealed by the test; and
      3. the Supplier’s proposals for remedying any such failures.
   6. Following each test, the Supplier shall take all measures requested by the Authority, (including requests for the re-testing of the Service Continuity Plan) to remedy any failures in the Service Continuity Plan and such remedial activity and re-testing shall be completed by the Supplier, at no additional cost to the Authority, by the date reasonably required by the Authority and set out in such notice.
   7. For the avoidance of doubt, the carrying out of a test of the Service Continuity Plan (including a test of the Service Continuity Plan’s procedures) shall not relieve the Supplier of any of its obligations under this Contract.
   8. The Supplier shall also perform a test of the Service Continuity Plan in the event of any major reconfiguration of the Services or as otherwise reasonably requested by the Authority.
3. Invocation of the Service Continuity Plan
   1. In the event of a loss of any critical part of the Service or a Disaster, the Supplier shall immediately invoke the business continuity and disaster recovery provisions in the Service Continuity Plan, including any linked elements in other parts of the Service Continuity Plan, and shall inform the Authority promptly of such invocation. In all other instances the Supplier shall invoke the business continuity and disaster recovery plan elements only with the prior consent of the Authority.
   2. The Insolvency Continuity Plan element of the Service Continuity Plans, including any linked elements in other parts of the Service Continuity Plan, shall be invoked by the Supplier:
      1. where an Insolvency Event of a Key Sub-contractor and/or Supplier Group member (other than the Supplier) could reasonably be expected to adversely affect delivery of the Services; and/or
      2. where there is an Insolvency Event of the Supplier and the insolvency arrangements enable the Supplier to invoke the plan;

## Part B: Corporate Resolution Planning

1. Service Status and Supplier Status
   1. The Supplier shall notify the Authority and the Cabinet Office Markets and Suppliers Team ([Resolution.planning@cabinetoffice.gov.uk](mailto:Resolution.planning@cabinetoffice.gov.uk)) in writing within 5 Working Days of the Effective Date and throughout the Term within 120 days after each Accounting Reference Date as to whether or not it is a Public Sector Dependent Supplier.
2. Provision of Corporate Resolution Planning Information (CRP Information)
   1. Paragraphs 2 to 4 of this Part B shall apply if this Contract has been specified by the Authority as a Critical Service Contract in section 9 *(Corporate Resolution Planning)* of the Front Sheet or the Supplier is or becomes a Public Sector Dependent Supplier.
   2. Subject to Paragraphs 2.6, 2.10 and 2.11 of this Part B:
      1. where this Contract is a Critical Service Contract, the Supplier shall provide the Relevant Authority or Relevant Authorities with CRP Information within 60 days of the Effective Date; and
      2. except where it has already been provided in accordance with Paragraph 2.2.1 of this Part B, where the Supplier is a Public Sector Dependent Supplier, it shall provide the Relevant Authority or Relevant Authorities with the CRP Information within 60 days of the date of the Relevant Authority’s or Relevant Authorities’ request.
   3. The Supplier shall ensure that the CRP Information provided pursuant to Paragraphs 2.2, 2.8 and 2.9 of this Part B:
      1. is full, comprehensive, accurate and up to date;
      2. is split into three parts:
         1. Exposure Information (Contracts List);
         2. Corporate Resolvability Assessment (Structural Review);
         3. Financial Information and Commentary

and is structured and presented in accordance with the requirements and explanatory notes set out at the relevant Annex of the latest published versions of the Resolution Planning Guidance Notes published by the Cabinet Office Government Commercial Function and available at <https://www.gov.uk/government/publications/the-sourcing-and-consultancy-playbooks> and contains the level of detail required (adapted as necessary to the Supplier’s circumstances);

* + 1. incorporates any additional commentary, supporting documents and evidence which would reasonably be required by the Relevant Authority or Relevant Authorities to understand and consider the information for approval;
    2. provides a clear description and explanation of the Supplier Group members that have agreements for goods, services or works provision in respect of UK Public Sector Business and/or CNI and the nature of those agreements; and
    3. complies with the requirements set out at Annex 1 (*Exposure Information (Contracts List)*), Annex 2 (*Corporate Resolvability Assessment (Structural Review)*) and Annex 3 (*Financial Information and Commentary*) respectively.
  1. Following receipt by the Relevant Authority or Relevant Authorities of the CRP Information pursuant to Paragraphs 2.2, 2.8 and 2.9 of this Part B, the Authority shall procure that the Relevant Authority or Relevant Authorities discuss in good faith the contents of the CRP Information with the Supplier and no later than 60 days after the date on which the CRP Information was delivered by the Supplier either provide an Assurance to the Supplier that Relevant Authority or Relevant Authorities approve the CRP Information or that Relevant Authority or Relevant Authorities reject the CRP Information.
  2. If the Relevant Authority or Relevant Authorities reject the CRP Information:
     1. the Authority shall (and shall procure that the Cabinet Office Markets and Suppliers Team shall) inform the Supplier in writing of its reasons for its rejection; and
     2. the Supplier shall revise the CRP Information, taking reasonable account of the Relevant Authority’s or Relevant Authorities’ comments, and shall re-submit the CRP Information to the Relevant Authority or Relevant Authorities for approval within 30 days of the date of the Relevant Authority’s or Relevant Authorities’ rejection. The provisions of Paragraph 2.3 to 2.5 of this Part B shall apply again to any resubmitted CRP Information provided that either Party may refer any disputed matters for resolution by the Dispute Resolution Procedure at any time.
  3. Where the Supplier or a member of the Supplier Group has already provided CRP Information to a Department or the Cabinet Office Markets and Suppliers Team (or, in the case of a Strategic Supplier, solely to the Cabinet Office Markets and Suppliers Team) and has received an Assurance of its CRP Information from that Department and the Cabinet Office Markets and Suppliers Team (or, in the case of a Strategic Supplier, solely from the Cabinet Office Markets and Suppliers Team), then provided that the Assurance remains Valid on the date by which the CRP Information would otherwise be required, the Supplier shall not be required to provide the CRP Information under Paragraph 2.2 if it provides a copy of the Valid Assurance to the Relevant Authority or Relevant Authorities on or before the date on which the CRP Information would otherwise have been required.
  4. An Assurance shall be deemed Valid for the purposes of Paragraph 2.6 of this Part B if:
     1. the Assurance is within the validity period stated in the Assurance (or, if no validity period is stated, no more than 12 months has elapsed since it was issued and no more than 18 months has elapsed since the Accounting Reference Date on which the CRP Information was based); and
     2. no Corporate Change Events or Financial Distress Events (or events which would be deemed to be Corporate Change Events or Financial Distress Events if this Contract had then been in force) have occurred since the date of issue of the Assurance.
  5. If this Contract is a Critical Service Contract, the Supplier shall provide an updated version of the CRP Information (or, in the case of Paragraph 2.8.3 of this Part B its initial CRP Information) to the Relevant Authority or Relevant Authorities:
     1. within 14 days of the occurrence of a Financial Distress Event (along with any additional highly confidential information no longer exempted from disclosure under Paragraph 2.11 of this Part B) unless the Supplier is relieved of the consequences of the Financial Distress Event under Paragraph 7.1 of Schedule 14 (*Financial Distress*)
     2. within 30 days of a Corporate Change Event unless:
        1. the Supplier requests and the Relevant Authority (acting reasonably) agrees to a Corporate Change Event Grace Period, in the event of which the time period for the Supplier to comply with this Paragraph shall be extended as determined by the Relevant Authority (acting reasonably) but shall in any case be no longer than six months after the Corporate Change Event. During a Corporate Change Event Grace Period the Supplier shall regularly and fully engage with the Relevant Authority to enable it to understand the nature of the Corporate Change Event and the Relevant Authority shall reserve the right to terminate a Corporate Change Event Grace Period at any time if the Supplier fails to comply with this Paragraph; or
        2. not required pursuant to Paragraph 2.10;
     3. within 30 days of the date that:
        1. the credit rating(s) of each of the Supplier and its Parent Undertakings fail to meet any of the criteria specified in Paragraph 2.10; or
        2. none of the credit rating agencies specified at Paragraph 2.10 hold a public credit rating for the Supplier or any of its Parent Undertakings; and
     4. in any event, within 6 months after each Accounting Reference Date or within 15 months of the date of the previous Assurance received from the Relevant Authority (whichever is the earlier), unless:
        1. updated CRP Information has been provided under any of Paragraphs 2.8.1 2.8.2 or 2.8.3 since the most recent Accounting Reference Date (being no more than 12 months previously) within the timescales that would ordinarily be required for the provision of that information under this Paragraph 2.8.4; or
        2. unless not required pursuant to Paragraph 2.10.
  6. Where the Supplier is a Public Sector Dependent Supplier and this Contract is not a Critical Service Contract, then on the occurrence of any of the events specified in Paragraphs 2.8.1 to 2.8.4 of this Part B, the Supplier shall provide at the request of the Relevant Authority or Relevant Authorities and within the applicable timescales for each event as set out in Paragraph 2.8 (or such longer timescales as may be notified to the Supplier by the Authority), the CRP Information to the Relevant Authority or Relevant Authorities.
  7. Where the Supplier or a Parent Undertaking of the Supplier has a credit rating of either:
     1. Aa3 or better from Moody’s; or
     2. AA- or better from Standard and Poor’s; or
     3. AA- or better from Fitch;

the Supplier will not be required to provide any CRP Information unless or until either (i) a Financial Distress Event occurs (unless the Supplier is relieved of the consequences of the Financial Distress Event under Paragraph 7.1 of Schedule 14 (*Financial Distress*)) or (ii) the Supplier and its Parent Undertakings cease to fulfil the criteria set out in this Paragraph 2.10, in which cases the Supplier shall provide the updated version of the CRP Information in accordance with Paragraph 2.8.

* 1. Subject to Paragraph 4, where the Supplier demonstrates to the reasonable satisfaction of the Relevant Authority or Relevant Authorities that a particular item of CRP Information is highly confidential, the Supplier may, having orally disclosed and discussed that information with the Relevant Authority or Relevant Authorities, redact or omit that information from the CRP Information provided that if a Financial Distress Event occurs, this exemption shall no longer apply and the Supplier shall promptly provide the relevant information to the Relevant Authority or Relevant Authorities to the extent required under Paragraph 2.8.

1. Termination Rights
   1. The Authority shall be entitled to terminate this Contract under Clause 31.1.2 (*Termination by the Authority*) if the Supplier is required to provide CRP Information under Paragraph 2 of this Part B and either:
      1. the Supplier fails to provide the CRP Information within 4 months of the Effective Date if this is a Critical Service Contract or otherwise within 4 months of the Relevant Authority’s or Relevant Authorities’ request; or
      2. the Supplier fails to obtain an Assurance from the Relevant Authority or Relevant Authorities within 4 months of the date that it was first required to provide the CRP Information under this Contract.
2. Confidentiality and usage of CRP Information
   1. The Authority agrees to keep the CRP Information confidential and use it only to understand the implications of an Insolvency Event of the Supplier and/or Supplier Group members on its UK Public Sector Business and/or services in respect of CNI and to enable contingency planning to maintain service continuity for end users and protect CNI in such eventuality.
   2. Where the Relevant Authority is the Cabinet Office Markets and Suppliers Team, at the Supplier’s request, the Authority shall use reasonable endeavours to procure that the Cabinet Office enters into a confidentiality and usage agreement with the Supplier containing terms no less stringent than those placed on the Authority under Paragraph 4.1 of this Part B and Clause 19 (*Confidentiality*).
   3. The Supplier shall use reasonable endeavours to obtain consent from any third party which has restricted the disclosure of the CRP Information to enable disclosure of that information to the Relevant Authority or Relevant Authorities pursuant to Paragraph 2 of this Part B subject, where necessary, to the Relevant Authority or Relevant Authorities entering into an appropriate confidentiality agreement in the form required by the third party.
   4. Where the Supplier is unable to procure consent pursuant to Paragraph 4.3 of this Part B, the Supplier shall use all reasonable endeavours to disclose the CRP Information to the fullest extent possible by limiting the amount of information it withholds including by:
      1. redacting only those parts of the information which are subject to such obligations of confidentiality
      2. providing the information in a form that does not breach its obligations of confidentiality including (where possible) by:
         1. summarising the information;
         2. grouping the information;
         3. anonymising the information; and
         4. presenting the information in general terms
   5. The Supplier shall provide the Relevant Authority or Relevant Authorities with contact details of any third party which has not provided consent to disclose CRP Information where that third party is also a public sector body and where the Supplier is legally permitted to do so.

## Annex 1: Exposure Information (Contracts List)

1. The Supplier shall:
   1. provide details of all agreements held by members of the Supplier Group where those agreements are for goods, services or works provision and:
      1. are with any UK public sector bodies including: Crown Bodies and their arms-length bodies and agencies, non-departmental public bodies, NHS bodies, local authorities, health bodies, police fire and rescue, education bodies and the devolved administrations;
      2. are with any private sector entities where the end recipient of the service, goods or works provision is any of the bodies set out in Paragraph 1.1.1 of this Annex 1 and where the member of the Supplier Group is acting as a key sub-contractor under the agreement with the end recipient; or
      3. involve or could reasonably be considered to involve CNI; and
   2. provide the Relevant Authority with a copy of the latest version of each underlying contract worth more than £5m per contract year and their related key sub-contracts, which shall be included as embedded documents within the CRP Information or via a directly accessible link.

## Annex 2: Corporate Resolvability Assessment (Structural Review)

1. The Supplier shall:
   1. provide sufficient information to allow the Relevant Authority to understand the implications on the Supplier Group’s UK Public Sector Business and CNI contracts listed pursuant to Annex 1 if the Supplier or another member of the Supplier Group is subject to an Insolvency Event.
   2. ensure that the information is presented so as to provide a simple, effective and easily understood overview of the Supplier Group; and
   3. provide full details of the importance of each member of the Supplier Group to the Supplier Group’s UK Public Sector Business and CNI contracts listed pursuant to Annex 1 and the dependencies between each.

## Annex 3: Financial Information and Commentary

1. The Supplier shall:
   1. provide sufficient financial information for the Supplier Group level, contracting operating entities level, and shared services entities’ level to allow the Relevant Authority to understand the current financial interconnectedness of the Supplier Group and the current performance of the Supplier as a standalone entity; and
   2. ensure that the information is presented in a simple, effective and easily understood manner.
2. For the avoidance of doubt the financial information to be provided pursuant to Paragraph 1 of this Annex 3 should be based on the most recent audited accounts for the relevant entities (or interim accounts where available) updated for any material changes since the Accounting Reference Date provided that such accounts are available in a reasonable timeframe to allow the Supplier to comply with its obligations under this Schedule 22 (*Service Continuity Plan and Corporate Resolution Planning*). If such accounts are not available in that timeframe, financial information should be based on unpublished unaudited accounts or management accounts (disclosure of which to the Cabinet Office Markets and Suppliers Team remains protected by confidentiality).

Schedule 27

Conduct of Claims

# Schedule 23: Conduct of Claims

1. Indemnities
   1. This Schedule shall apply to the conduct, by a Party from whom an indemnity is sought under this Contract (the “Indemnifier”), of claims made by a third person against a party having (or claiming to have) the benefit of the indemnity (the “Beneficiary”).
   2. If the Beneficiary receives any notice of any claim for which it appears that the Beneficiary is, or may become, entitled to indemnification under this Contract (a “Claim”), the Beneficiary shall give notice in writing to the Indemnifier as soon as reasonably practicable and in any event within 10 Working Days of receipt of the same.
   3. Subject to Paragraph 2, on the giving of a notice by the Beneficiary, where it appears that the Beneficiary is or may be entitled to indemnification from the Indemnifier in respect of all (but not part only) of the liability arising out of the Claim, the Indemnifier shall (subject to providing the Beneficiary with a secured indemnity to its reasonable satisfaction against all costs and expenses that it may incur by reason of such action) be entitled to dispute the Claim in the name of the Beneficiary at the Indemnifier’s own expense and take conduct of any defence, dispute, compromise or appeal of the Claim and of any incidental negotiations relating to the Claim. If the Indemnifier does elect to conduct the Claim, the Beneficiary shall give the Indemnifier all reasonable cooperation, access and assistance for the purposes of such Claim and, subject to Paragraph 2.2, the Beneficiary shall not make any admission which could be prejudicial to the defence or settlement of the Claim without the prior written consent of the Indemnifier.
   4. With respect to any Claim conducted by the Indemnifier pursuant to Paragraph 1.3:
      1. the Indemnifier shall keep the Beneficiary fully informed and consult with it about material elements of the conduct of the Claim;
      2. the Indemnifier shall not bring the name of the Beneficiary into disrepute;
      3. the Indemnifier shall not pay or settle such Claim without the prior written consent of the Beneficiary, such consent not to be unreasonably withheld or delayed; and
      4. the Indemnifier shall conduct the Claim with all due diligence.
   5. The Beneficiary shall be entitled to have conduct of the Claim and shall be free to pay or settle any Claim on such terms as it thinks fit and without prejudice to its rights and remedies under this Contract if:
      1. the Indemnifier is not entitled to take conduct of the Claim in accordance with Paragraph 1.3;
      2. the Indemnifier fails to notify the Beneficiary in writing of its intention to take conduct of the relevant Claim within 10 Working Days of the notice from the Beneficiary or if the Indemnifier notifies the Beneficiary in writing that it does not intend to take conduct of the Claim; or
      3. the Indemnifier fails to comply in any material respect with the provisions of Paragraph 1.4.
2. Sensitive Claims
   1. With respect to any Claim which the Beneficiary, acting reasonably, considers is likely to have an adverse impact on the general public’s perception of the Beneficiary (a “Sensitive Claim”), the Indemnifier shall be entitled to take conduct of any defence, dispute, compromise or appeal of the Sensitive Claim only with the Beneficiary’s prior written consent. If the Beneficiary withholds such consent and elects to conduct the defence, dispute, compromise or appeal of the Sensitive Claim itself, it shall conduct the Sensitive Claim with all due diligence and if it fails to do so, the Indemnifier shall only be liable to indemnify the Beneficiary in respect of that amount which would have been recoverable by the Beneficiary had it conducted the Sensitive Claim with all due diligence.
   2. The Beneficiary shall be free at any time to give written notice to the Indemnifier that it is retaining or taking over (as the case may be) the conduct of any Claim, to which Paragraph 1.3 applies if, in the reasonable opinion of the Beneficiary, the Claim is, or has become, a Sensitive Claim.
3. Recovery of Sums
   1. If the Indemnifier pays to the Beneficiary an amount in respect of an indemnity and the Beneficiary subsequently recovers (whether by payment, discount, credit, saving, relief or other benefit or otherwise) a sum which is directly referable to the fact, matter, event or circumstances giving rise to the Claim, the Beneficiary shall forthwith repay to the Indemnifier whichever is the lesser of:
      1. an amount equal to the sum recovered (or the value of the discount, credit, saving, relief, other benefit or amount otherwise obtained) less any out-of-pocket costs and expenses properly incurred by the Beneficiary in recovering or obtaining the same; and
      2. the amount paid to the Beneficiary by the Indemnifier in respect of the Claim under the relevant indemnity.
4. Mitigation
   1. Each of the Authority and the Supplier shall at all times take all reasonable steps to minimise and mitigate any loss for which the relevant Party is entitled to bring a claim against the other Party pursuant to the indemnities in this Schedule.

Schedule 24

Staff Transfer

# Schedule 24: Staff Transfer

***[Guidance: Authorities will need to take their own legal advice on this Schedule 24 and, in particular, on Part D*** ***(Pensions).***

***Authorities will need to ensure that appropriate provisions are included to deal with staff transfer on both entry and exit. Irrespective of whether TUPE does apply on entry if there are employees eligible for New Fair Deal pension protection then the appropriate pensions provisions will also need to be selected.***

***If there is a staff transfer from the Authority on entry (1st generation) then Part A shall apply.***

***If there is a staff transfer from former/incumbent supplier on entry (2nd generation), Part B shall apply. Part B contains an obligation on the Authority to procure indemnities from a Former Supplier in so far as it is reasonably able to do. Legal advice is recommended if using this Part B.***

***If there is both a 1st and 2nd generation staff transfer on entry, then both Part A and Part B shall apply.***

***If the Parties agree that TUPE is not expected to apply at the Operational Service Commencement Date, on either a 1st generation or a 2nd generation transfer, then Part C shall apply. In Part C the Authority is stating that it believes TUPE will not apply and is both (i) giving indemnities and (ii) agreeing to procure indemnities from the Former Supplier, should this prove incorrect and TUPE does apply. Legal advice should be sought before the Authority gives such indemnities/uses Part C.***

***Part D*** ***(Pensions) may also apply should staff transfer or claim to have transferred.***

***Part D will apply where Part A applies, is likely to apply where Part B applies, and may apply where Part C applies. Please note that Part D may also apply where there is not a TUPE transfer, for example, where the incumbent provider is successful and becomes the new Supplier. Authorities will need to select which Annex shall apply (either Annex D1 (CSPS), Annex D2 (NHSPS), Annex D3 (LGPS) or Annex D4 (Other Schemes)).***

***Please note that the Authority is giving indemnities in Part A and C, and is agreeing to procure indemnities in Part B, Part C, and Part E. Legal advice is required, therefore, to ensure that the Authority understands the scope of its liability under these indemnities.***

***Please note the MSC at Part E contains exit provisions and indemnities including, at Part E Paragraph 2.12, the obligation on the Authority to procure indemnities from a Replacement Supplier in favour of the Supplier. If the Authority is co-commissioning these Services or commissioning on behalf of another part of the Crown, consideration should be given as to whether the Authority will be able to procure such indemnities or whether the obligation should be to use “reasonable endeavours” to procure.***

***Part E (dealing with staff transfer on exit) shall apply to every Contract, even if TUPE does not apply on entry.***

***Please also note that in relation to ELI information in Part E, the Exit Management Schedule (Schedule 21) provides that the Supplier may charge the Authority for its reasonable additional costs to the extent the Authority requests more than 4 updates to 'Exit Information' in any 6 month period.***

***Note that some paragraphs of this Schedule are referred to in the "Third Party Rights" section of the Core Terms, and care should be taken to update these references if there is any renumbering in this Schedule.***

***For Central Government Authorities further guidance on this Schedule contact Government Legal Department’s Employment Law Group]***

1. Definitions
   1. In this Schedule, the following definitions shall apply:

|  |  |
| --- | --- |
| “Admission Agreement” | either or both of the CSPS Admission Agreement (as defined in Annex D1: CSPS) or the LGPS Admission Agreement) as defined in Annex D3: LGPS), as the context requiresas; |
| “Fair Deal Employees” | as defined in Part D; |
| "Final Supplier Personnel List" | a list provided by the Supplier of all Supplier Personnel who will transfer under the Employment Regulations on the Service Transfer Date; |
| “Former Supplier” | a supplier supplying services to the Authority before any Relevant Transfer Date that are the same as or substantially similar to the Services (or any part of the Services) and shall include any sub-contractor of such supplier (or any sub-contractor of any such sub-contractor); |
| “New Fair Deal” | the revised Fair Deal position set out in the HM Treasury guidance: *“Fair Deal for Staff Pensions: Staff Transfer from Central Government”* issued in October 2013 including:   1. any amendments to that document immediately prior to the Relevant Transfer Date; 2. any similar pension protection in accordance with the subsequent Annexes D1-D3 inclusive as notified to the Supplier by the Authority; |
| “Notified Sub-contractor” | a Sub-contractor identified in the Annex to this Schedule to whom Transferring Authority Employees and/or Transferring Former Supplier Employees will transfer on a Relevant Transfer Date; |
| “Old Fair Deal” | HM Treasury Guidance *“Staff Transfers from Central Government: A Fair Deal for Staff Pensions”* issued in June 1999 including the supplementary guidance *“Fair Deal for Staff pensions: Procurement of Bulk Transfer Agreements and Related Issues”* issued in June 2004; |
| "Provisional Supplier Personnel List" | a list prepared and updated by the Supplier of all Supplier Personnel who are at the date of the list wholly or mainly engaged in or assigned to the provision of the Services or any relevant part of the Services which it is envisaged as at the date of such list will no longer be provided by the Supplier; |
| “Replacement Sub-contractor” | a sub-contractor of the Replacement Supplier to whom Transferring Supplier Employees will transfer on a Service Transfer Date (or any sub-contractor of any such sub-contractor); |
| “Relevant Transfer” | a transfer of employment to which the Employment Regulations applies; |
| “Relevant Transfer Date” | in relation to a Relevant Transfer, the date upon which the Relevant Transfer takes place. For the purposes of Part D and its Annexes, where the Supplier or a Sub-contractor was the Former Supplier and there is no Relevant Transfer of the Fair Deal Employees because they remain continuously employed by the Supplier (or Sub-contractor), references to the Relevant Transfer Date shall become references to the Operational Service Commencement Date; |
| “Service Transfer” | any transfer of the Services (or any part of the Services), for whatever reason, from the Supplier or any Sub-contractor to a Replacement Supplier or a Replacement Sub-contractor; |
| “Service Transfer Date” | the date of a Service Transfer or, if more than one, the date of the relevant Service Transfer as the context requires; |
| “Staffing Information” | in relation to all persons identified on the Provisional Supplier Personnel List or Final Supplier Personnel List, as the case may be, the information required in Annex E2: Staffing Information in that format together with employee liability information specified in Regulation 11(2) and 11(3) and if applicable 11(4) of the Employment Regulations and such other information as the Authority may reasonably require. The Authority may acting reasonably make changes to the format or information requested in Annex E2: Staffing Information from time to time; |
| “Statutory Schemes” | means the CSPS, NHSPS or LGPS as defined in the Annexes to Part D of this Schedule; |
| “Transferring Authority Employees” | those employees of the Authority to whom the Employment Regulations will apply on the Relevant Transfer Date; |
| “Transferring Former Supplier Employees” | in relation to a Former Supplier, those employees of the Former Supplier to whom the Employment Regulations will apply on the Relevant Transfer Date; and |
| “Transferring Supplier Employees” | those employees of the Supplier and/or the Supplier’s Sub-contractors to whom the Employment Regulations will apply on the Service Transfer Date. |

1. Interpretation
   1. Where a provision in this Schedule imposes an obligation on the Supplier to provide an indemnity, undertaking or warranty, the Supplier shall procure that each of its Sub-contractors shall comply with such obligation and provide such indemnity, undertaking or warranty to the Authority, Former Supplier, Replacement Supplier or Replacement Sub-contractor, as the case may be.
2. Applicable Parts of this Schedule
   1. The only applicable Part(s) of this Schedule are as selected by the Authority in Section 10 (Staff Transfer) of the Front Sheet.

## Part A: Transferring Authority Employees at Commencement of Services

1. Relevant Transfers
   1. The Authority and the Supplier agree that:
      1. the commencement of the provision of the Services or of each relevant part of the Services will be a Relevant Transfer in relation to the Transferring Authority Employees; and
      2. as a result of the operation of the Employment Regulations, the contracts of employment between the Authority and the Transferring Authority Employees (except in relation to any terms disapplied through operation of regulation 10 of the Employment Regulations) will have effect on and from the Relevant Transfer Date as if originally made between the Supplier and/or any Notified Sub-contractor and each such Transferring Authority Employee.
   2. The Authority shall comply with all its obligations under the Employment Regulations and shall perform and discharge all its obligations in respect of the Transferring Authority Employees in respect of the period arising up to (but not including)the Relevant Transfer Date (including the payment of all remuneration, benefits, entitlements and outgoings, all wages, accrued but untaken holiday pay, bonuses, commissions, payments of PAYE, national insurance contributions and pension contributions which in any case are attributable in whole or in part to the period up to (but not including) the Relevant Transfer Date) and any necessary apportionments in respect of any periodic payments shall be made between: (i) the Authority; and (ii) the Supplier and/or any Notified Sub-contractor (as appropriate).
2. Authority Indemnities
   1. Subject to Paragraph 2.2, the Authority shall indemnify the Supplier and any Notified Sub-contractor against any Employee Liabilities arising from or as a result of:
      1. any act or omission by the Authority in respect of any Transferring Authority Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Authority Employee occurring before the Relevant Transfer Date;
      2. the breach or non-observance by the Authority before the Relevant Transfer Date of:
         1. any collective agreement applicable to the Transferring Authority Employees; and/or
         2. any custom or practice in respect of any Transferring Authority Employees which the Authority is contractually bound to honour;
      3. any claim by any trade union or other body or person representing the Transferring Authority Employees arising from or connected with any failure by the Authority to comply with any legal obligation to such trade union, body or person arising before the Relevant Transfer Date;
      4. any proceeding, claim or demand by HMRC or other statutory authority in respect of any financial obligation including, but not limited to, PAYE and primary and secondary national insurance contributions:
         1. in relation to any Transferring Authority Employee, to the extent that the proceeding, claim or demand by HMRC or other statutory authority relates to financial obligations arising before the Relevant Transfer Date; and
         2. in relation to any employee who is not a Transferring Authority Employee and in respect of whom it is later alleged or determined that the Employment Regulations applied so as to transfer his/her employment from the Authority to the Supplier and/or any Notified Sub-contractor as appropriate, to the extent that the proceeding, claim or demand by the HMRC or other statutory authority relates to financial obligations arising before the Relevant Transfer Date.
      5. a failure of the Authority to discharge, or procure the discharge of, all wages, salaries and all other benefits and all PAYE tax deductions and national insurance contributions relating to the Transferring Authority Employees arising before the Relevant Transfer Date;
      6. any claim made by or in respect of any person employed or formerly employed by the Authority other than a Transferring Authority Employee for whom it is alleged the Supplier and/or any Notified Sub-contractor as appropriate may be liable by virtue of the Employment Regulations; and
      7. any claim made by or in respect of a Transferring Authority Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Authority Employee relating to any act or omission of the Authority in relation to its obligations under regulation 13 of the Employment Regulations, except to the extent that the liability arises from the failure by the Supplier or any Sub-contractor to comply with regulation 13(4) of the Employment Regulations.
   2. The indemnities in Paragraph 2.1 shall not apply to the extent that the Employee Liabilities arise or are attributable to an act or omission of the Supplier or any Sub-contractor (whether or not a Notified Sub-contractor) whether occurring or having its origin before, on or after the Relevant Transfer Date including any Employee Liabilities:
      1. arising out of the resignation of any Transferring Authority Employee before the Relevant Transfer Date on account of substantial detrimental changes to his/her working conditions proposed by the Supplier and/or any Sub-contractor to occur in the period from (and including) the Relevant Transfer Date; or
      2. arising from the failure by the Supplier or any Sub-contractor to comply with its obligations under the Employment Regulations.
   3. If any person who is not identified by the Authority as a Transferring Authority Employee claims, or it is determined in relation to any person who is not identified by the Authority as a Transferring Authority Employee, that his/her contract of employment has been transferred from the Authority to the Supplier and/or any Notified Sub-contractor pursuant to the Employment Regulations then:
      1. the Supplier shall, or shall procure that the Notified Sub-contractor shall, within 5 Working Days of becoming aware of that fact, give notice in writing to the Authority; and
      2. the Authority may offer (or may procure that a third party may offer) employment to such person within 15 Working Days of receipt of the notification by the Supplier and/or any Notified Sub-contractor, or take such other reasonable steps as the Authority considers appropriate to deal with the matter provided always that such steps are in compliance with Law.
   4. If an offer referred to in Paragraph 2.3.2 is accepted, or if the situation has otherwise been resolved by the Authority, the Supplier shall, or shall procure that the Notified Sub-contractor shall, immediately release the person from his/her employment or alleged employment.
   5. If by the end of the 15 Working Day period specified in Paragraph 2.3.2:
      1. no such offer of employment has been made;
      2. such offer has been made but not accepted; or
      3. the situation has not otherwise been resolved,

the Supplier and/or any Notified Sub-contractor may within 5 Working Days give notice to terminate the employment or alleged employment of such person.

* 1. Subject to the Supplier and/or any Notified Sub-contractor acting in accordance with the provisions of Paragraphs 2.3 to 2.5 and in accordance with all applicable proper employment procedures set out in applicable Law, the Authority shall indemnify the Supplier and/or any Notified Sub-contractor (as appropriate) against all Employee Liabilities arising out of the termination of employment pursuant to the provisions of Paragraph 2.5 provided that the Supplier takes, or procures that the Notified Sub-contractor takes, all reasonable steps to minimise any such Employee Liabilities.
  2. The indemnity in Paragraph 2.6:
     1. shall not apply to:
        1. any claim for:

(i) any contravention of the Equality Act 2010 (or predecessor/successor legislation); or

(ii) equal pay or compensation for less favourable treatment of part-time workers or fixed-term employees,

in any case in relation to any alleged act or omission of the Supplier and/or any Sub-contractor; or

* + - 1. any claim that the termination of employment was unfair because the Supplier and/or Notified Sub-contractor neglected to follow a fair dismissal procedure; and
    1. shall apply only where the notification referred to in Paragraph 2.3.1 is made by the Supplier and/or any Notified Sub-contractor (as appropriate) to the Authority within 6 months of the Relevant Transfer Date.
  1. If any such person as is referred to in Paragraph 2.3 is neither re-employed by the Authority nor dismissed by the Supplier and/or any Notified Sub-contractor within the time scales set out in Paragraph 2.5 such person shall be treated as having transferred to the Supplier and/or any Notified Sub-contractor and the Supplier shall, or shall procure that the Notified Sub-contractor shall, (a) comply with such obligations as may be imposed upon it under applicable Law and (b) comply with the provisions of Part D (Pensions) and its Annexes of this Staff Transfer Schedule.

1. Supplier Indemnities and Obligations
   1. Subject to Paragraph 3.2, the Supplier shall indemnify the Authority against any Employee Liabilities arising from or as a result of:
      1. any act or omission by the Supplier or any Sub-contractor in respect of any Transferring Authority Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Authority Employee whether occurring before, on or after the Relevant Transfer Date;
      2. the breach or non-observance by the Supplier or any Sub-contractor on or after the Relevant Transfer Date of:
         1. any collective agreement applicable to the Transferring Authority Employees; and/or
         2. any custom or practice in respect of any Transferring Authority Employees which the Supplier or any Sub-contractor is contractually bound to honour;
      3. any claim by any trade union or other body or person representing any Transferring Authority Employees arising from or connected with any failure by the Supplier or any Sub-contractor to comply with any legal obligation to such trade union, body or person arising on or after the Relevant Transfer Date;
      4. any proposal by the Supplier or a Sub-contractor made before the Relevant Transfer Date to make changes to the terms and conditions of employment or working conditions of any Transferring Authority Employees to their material detriment on or after their transfer to the Supplier or the relevant Sub-contractor (as the case may be) on the Relevant Transfer Date, or to change the terms and conditions of employment or working conditions of any person who would have been a Transferring Authority Employee but for their resignation (or decision to treat their employment as terminated under regulation 4(9) of the Employment Regulations) before the Relevant Transfer Date as a result of or for a reason connected to such proposed changes;
      5. any statement communicated to or action undertaken by the Supplier or any Sub-contractor to, or in respect of, any Transferring Authority Employee before the Relevant Transfer Date regarding the Relevant Transfer which has not been agreed in advance with the Authority in writing;
      6. any proceeding, claim or demand by HMRC or other statutory authority in respect of any financial obligation including, but not limited to, PAYE and primary and secondary national insurance contributions:
         1. in relation to any Transferring Authority Employee, to the extent that the proceeding, claim or demand by HMRC or other statutory authority relates to financial obligations arising on or after the Relevant Transfer Date; and
         2. in relation to any employee who is not a Transferring Authority Employee, and in respect of whom it is later alleged or determined that the Employment Regulations applied so as to transfer his/her employment from the Authority to the Supplier or a Sub-contractor, to the extent that the proceeding, claim or demand by HMRC or other statutory authority relates to financial obligations arising on or after the Relevant Transfer Date;
      7. a failure of the Supplier or any Sub-contractor to discharge or procure the discharge of all wages, salaries and all other benefits and all PAYE tax deductions and national insurance contributions relating to the Transferring Authority Employees in respect of the period from (and including) the Relevant Transfer Date;
      8. any claim made by or in respect of a Transferring Authority Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Authority Employee relating to any act or omission of the Supplier or any Sub-contractor in relation to their obligations under regulation 13 of the Employment Regulations, except to the extent that the liability arises from the Authority’s failure to comply with its obligations under regulation 13 of the Employment Regulations; and
      9. a failure by the Supplier or any Sub-Contractor to comply with its obligations under Paragraph 2.8 above.
   2. The indemnities in Paragraph 3.1 shall not apply to the extent that the Employee Liabilities arise or are attributable to an act or omission of the Authority whether occurring or having its origin before, on or after the Relevant Transfer Date including, without limitation, any Employee Liabilities arising from the Authority’s failure to comply with its obligations under the Employment Regulations.
   3. The Supplier shall comply, and shall procure that each Sub-contractor shall comply, with all its obligations under the Employment Regulations (including its obligation to inform and consult in accordance with regulation 13 of the Employment Regulations) and shall perform and discharge, and shall procure that each Sub-contractor shall perform and discharge, all its obligations in respect of the Transferring Authority Employees, from (and including) the Relevant Transfer Date (including the payment of all remuneration, benefits, entitlements and outgoings, all wages, accrued but untaken holiday pay, bonuses, commissions, payments of PAYE, national insurance contributions and pension contributions and any other sums due under the Admission Agreement which in any case are attributable in whole or in part to the period from and including the Relevant Transfer Date) and any necessary apportionments in respect of any periodic payments shall be made between the Authority and the Supplier.
2. Information
   1. The Supplier shall, and shall procure that each Sub-contractor shall, promptly provide to the Authority in writing such information as is necessary to enable the Authority to carry out its duties under regulation 13 of the Employment Regulations. The Authority shall promptly provide to the Supplier and each Notified Sub-contractor in writing such information as is necessary to enable the Supplier and each Notified Sub-contractor to carry out their respective duties under regulation 13 of the Employment Regulations.
3. Principles of Good Employment Practice
   1. The Parties agree that the Principles of Good Employment Practice issued by the Cabinet Office in December 2010 apply to the treatment by the Supplier of employees whose employment begins after the Relevant Transfer Date, and the Supplier undertakes to treat such employees in accordance with the provisions of the Principles of Good Employment Practice.
   2. The Supplier shall, and shall procure that each Sub-contractor shall, comply with any requirement notified to it by the Authority relating to pensions in respect of any Transferring Authority Employee as set down in:
      1. the Cabinet Office Statement of Practice on Staff Transfers in the Public Sector of January 2000, revised December 2013;
      2. Old Fair Deal; and/or
      3. the New Fair Deal.
   3. The Supplier acknowledges, in respect of those Transferring Authority Employees who were eligible for compensation under the terms of Civil Service Compensation Scheme (“**CSCS**”) immediately prior to transfer, that the right to benefits calculated in accordance with the terms of the CSCS will transfer under the Employment Regulations. The Supplier acknowledges and accepts that for any employee who was eligible for compensation under or in accordance with the terms of the CSCS, the right to compensation, is a right to compensation in accordance with the terms of the CSCS applicable at the time at which the employee becomes entitled to such compensation (including voluntary or compulsory redundancy). Suppliers are advised to check the Civil Service Pensions website for the current CSCS terms.
   4. Any changes necessary to this Contract as a result of changes to, or any replacement of any statement of practice, paper or other guidance that replaces any of the documentation referred to in Paragraphs 5.1 or 5.2 shall be agreed in accordance with the Change Control Procedure.
4. Pensions
   1. The Supplier shall, and/or shall procure that each of its Sub-contractors shall, comply with:
      1. the requirements of Part 1 of the Pensions Act 2008, section 258 of the Pensions Act 2004 and the Transfer of Employment (Pension Protection) Regulations 2005 for all transferring staff; and
      2. Part D (and its Annexes) to this Staff Transfer Schedule.

## Part B: Transferring Former Supplier Employees at Commencement of Services

1. Relevant Transfers
   1. The Authority and the Supplier agree that:
      1. the commencement of the provision of the Services or of any relevant part of the Services will be a Relevant Transfer in relation to the Transferring Former Supplier Employees; and
      2. as a result of the operation of the Employment Regulations, the contracts of employment between each Former Supplier and the Transferring Former Supplier Employees (except in relation to any terms disapplied through the operation of regulation 10 of the Employment Regulations) shall have effect on and from the Relevant Transfer Date as if originally made between the Supplier and/or Notified Sub-contractor and each such Transferring Former Supplier Employee.
   2. The Authority shall procure that each Former Supplier shall comply with all its obligations under the Employment Regulations and shall perform and discharge all its obligations in respect of all the Transferring Former Supplier Employees in respect of the period up to (but not including) the Relevant Transfer Date (including the payment of all remuneration, benefits, entitlements and outgoings, all wages, accrued but untaken holiday pay, bonuses, commissions, payments of PAYE, national insurance contributions and pension contributions which in any case are attributable in whole or in part in respect of the period up to (but not including) the Relevant Transfer Date) and the Supplier shall make, and the Authority shall procure that each Former Supplier makes, any necessary apportionments in respect of any periodic payments.
2. Former Supplier Indemnities
   1. Subject to Paragraph 2.2, the Authority shall procure that each Former Supplier shall indemnify the Supplier and any Notified Sub-contractor against any Employee Liabilities arising from or as a result of:
      1. any act or omission by the Former Supplier in respect of any Transferring Former Supplier Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Former Supplier Employee arising before the Relevant Transfer Date;
      2. the breach or non-observance by the Former Supplier arising before the Relevant Transfer Date of:
         1. any collective agreement applicable to the Transferring Former Supplier Employees; and/or
         2. any custom or practice in respect of any Transferring Former Supplier Employees which the Former Supplier is contractually bound to honour;
      3. any proceeding, claim or demand by HMRC or other statutory authority in respect of any financial obligation including, but not limited to, PAYE and primary and secondary national insurance contributions:
         1. in relation to any Transferring Former Supplier Employee, to the extent that the proceeding, claim or demand by HMRC or other statutory authority relates to financial obligations arising before the Relevant Transfer Date; and
         2. in relation to any employee who is not a Transferring Former Supplier Employee and in respect of whom it is later alleged or determined that the Employment Regulations applied so as to transfer his/her employment from the Former Supplier to the Supplier and/or any Notified Sub-contractor as appropriate, to the extent that the proceeding, claim or demand by HMRC or other statutory authority relates to financial obligations in respect of the period to (but excluding) the Relevant Transfer Date;
      4. a failure of the Former Supplier to discharge or procure the discharge of all wages, salaries and all other benefits and all PAYE tax deductions and national insurance contributions relating to the Transferring Former Supplier Employees in respect of the period to (but excluding) the Relevant Transfer Date;
      5. any claim made by or in respect of any person employed or formerly employed by the Former Supplier other than a Transferring Former Supplier Employee for whom it is alleged the Supplier and/or any Notified Sub-contractor as appropriate may be liable by virtue of this Contract and/or the Employment Regulations; and
      6. any claim made by or in respect of a Transferring Former Supplier Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Former Supplier Employee relating to any act or omission of the Former Supplier in relation to its obligations under regulation 13 of the Employment Regulations, except to the extent that the liability arises from the failure by the Supplier or any Sub-contractor to comply with regulation 13(4) of the Employment Regulations.
   2. The indemnities in Paragraph 2.1 shall not apply to the extent that the Employee Liabilities arise or are attributable to an act or omission of the Supplier or any Sub-contractor whether occurring or having its origin before, on or after the Relevant Transfer Date including, without limitation, any Employee Liabilities:
      1. arising out of the resignation of any Transferring Former Supplier Employee before the Relevant Transfer Date on account of substantial detrimental changes to his/her working conditions proposed by the Supplier or any Sub-contractor to occur in the period from (and including) the Relevant Transfer Date; or
      2. arising from the failure by the Supplier and/or any Sub-contractor to comply with its obligations under the Employment Regulations.
   3. If any person who is not identified as a Transferring Former Supplier Employee claims, or it is determined in relation to any person who is not identified as a Transferring Former Supplier Employee, that his/her contract of employment has been transferred from a Former Supplier to the Supplier and/or any Notified Sub-contractor pursuant to the Employment Regulations then:
      1. the Supplier shall, or shall procure that the Notified Sub-contractor shall, within 5 Working Days of becoming aware of that fact, give notice in writing to the Authority and, where required by the Authority, to the Former Supplier; and
      2. the Former Supplier may offer (or may procure that a third party may offer) employment to such person within 15 Working Days of the notification by the Supplier and/or the Notified Sub-contractor or take such other reasonable steps as the Former Supplier considers appropriate to deal with the matter provided always that such steps are in compliance with applicable Law.
   4. If an offer referred to in Paragraph 2.3.2 is accepted, or if the situation has otherwise been resolved by the Former Supplier and/or the Authority, the Supplier shall, or shall procure that the Notified Sub-contractor shall, immediately release the person from his/her employment or alleged employment.
   5. If by the end of the 15 Working Day period specified in Paragraph 2.3.2:
      1. no such offer of employment has been made;
      2. such offer has been made but not accepted; or
      3. the situation has not otherwise been resolved,

the Supplier and/or any Notified Sub-contractor may within 5 Working Days give notice to terminate the employment or alleged employment of such person.

* 1. Subject to the Supplier and/or any Notified Sub-contractor acting in accordance with the provisions of Paragraphs 2.3 to 2.5 and in accordance with all applicable proper employment procedures set out in Law, the Authority shall procure that the Former Supplier indemnifies the Supplier and/or any Notified Sub-contractor (as appropriate) against all Employee Liabilities arising out of the termination of employment pursuant to the provisions of Paragraph 2.5 provided that the Supplier takes, or shall procure that the Notified Sub-contractor takes, all reasonable steps to minimise any such Employee Liabilities.
  2. The indemnity in Paragraph 2.6:
     1. shall not apply to:
        1. any claim for:

(i) any contravention of the Equality Act 2010 (or predecessor/successor legislation); or

(ii) equal pay or compensation for less favourable treatment of part-time workers or fixed-term employees,

in any case in relation to any alleged act or omission of the Supplier and/or any Sub-contractor; or

* + - 1. any claim that the termination of employment was unfair because the Supplier and/or Notified Sub-contractor neglected to follow a fair dismissal procedure; and
    1. shall apply only where the notification referred to in Paragraph 2.3.1 is made by the Supplier and/or any Notified Sub-contractor (as appropriate) to the Authority and, if applicable, the Former Supplier, within 6 months of the Relevant Transfer Date.
  1. If any such person as is described in Paragraph 2.3 is neither re-employed by the Former Supplier nor dismissed by the Supplier and/or any Notified Sub-contractor within the time scales set out in Paragraph 2.5, such person shall be treated as having transferred to the Supplier or Notified Sub-contractor and the Supplier shall, or shall procure that the Notified Sub-contractor shall, (a) comply with such obligations as may be imposed upon it under the Law and (b) comply with the provisions of Part D (*Pensions*) and its Annexes of this Staff Transfer Schedule.

1. Supplier Indemnities and Obligations
   1. Subject to Paragraph 3.2, the Supplier shall indemnify the Authority and/or the Former Supplier against any Employee Liabilities arising from or as a result of:
      1. any act or omission by the Supplier or any Sub-contractor in respect of any Transferring Former Supplier Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Former Supplier Employee whether occurring before, on or after the Relevant Transfer Date;
      2. the breach or non-observance by the Supplier or any Sub-contractor on or after the Relevant Transfer Date of:
         1. any collective agreement applicable to the Transferring Former Supplier Employee; and/or
         2. any custom or practice in respect of any Transferring Former Supplier Employees which the Supplier or any Sub-contractor is contractually bound to honour;
      3. any claim by any trade union or other body or person representing any Transferring Former Supplier Employees arising from or connected with any failure by the Supplier or a Sub-contractor to comply with any legal obligation to such trade union, body or person arising on or after the Relevant Transfer Date;
      4. any proposal by the Supplier or a Sub-contractor prior to the Relevant Transfer Date to make changes to the terms and conditions of employment or working conditions of any Transferring Former Supplier Employees to their material detriment on or after their transfer to the Supplier or a Sub-contractor (as the case may be) on the Relevant Transfer Date, or to change the terms and conditions of employment or working conditions of any person who would have been a Transferring Former Supplier Employee but for their resignation (or decision to treat their employment as terminated under regulation 4(9) of the Employment Regulations) before the Relevant Transfer Date as a result of or for a reason connected to such proposed changes;
      5. any statement communicated to or action undertaken by the Supplier or a Sub-contractor to, or in respect of, any Transferring Former Supplier Employee before the Relevant Transfer Date regarding the Relevant Transfer which has not been agreed in advance with the Authority and/or the Former Supplier in writing;
      6. any proceeding, claim or demand by HMRC or other statutory authority in respect of any financial obligation including, but not limited to, PAYE and primary and secondary national insurance contributions:
         1. in relation to any Transferring Former Supplier Employee, to the extent that the proceeding, claim or demand by HMRC or other statutory authority relates to financial obligations arising on or after the Relevant Transfer Date; and
         2. in relation to any employee who is not a Transferring Former Supplier Employee, and in respect of whom it is later alleged or determined that the Employment Regulations applied so as to transfer his/her employment from the Former Supplier to the Supplier or a Sub-contractor, to the extent that the proceeding, claim or demand by the HMRC or other statutory authority relates to financial obligations arising on or after the Relevant Transfer Date;
      7. a failure of the Supplier or any Sub-contractor to discharge or procure the discharge of all wages, salaries and all other benefits and all PAYE tax deductions and national insurance contributions relating to the Transferring Former Supplier Employees in respect of the period from (and including) the Relevant Transfer Date;
      8. any claim made by or in respect of a Transferring Former Supplier Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Former Supplier Employee relating to any act or omission of the Supplier or any Sub-contractor in relation to obligations under regulation 13 of the Employment Regulations, except to the extent that the liability arises from the Former Supplier’s failure to comply with its obligations under regulation 13(4) of the Employment Regulations; and
      9. a failure by the Supplier or any Sub-Contractor to comply with its obligations under Paragraph 2.8 above
   2. The indemnities in Paragraph 3.1 shall not apply to the extent that the Employee Liabilities arise or are attributable to an act or omission of the Former Supplier whether occurring or having its origin before, on or after the Relevant Transfer Date including, without limitation, any Employee Liabilities arising from the Former Supplier’s failure to comply with its obligations under the Employment Regulations.
   3. The Supplier shall comply, and shall procure that each Sub-contractor shall comply, with all its obligations under the Employment Regulations (including without limitation its obligation to inform and consult in accordance with regulation 13 of the Employment Regulations) and shall perform and discharge, and shall procure that each Sub-contractor shall perform and discharge, all its obligations in respect of all the Transferring Former Supplier Employees, on and from the Relevant Transfer Date (including the payment of all remuneration, benefits, entitlements and outgoings, all wages, accrued but untaken holiday pay, bonuses, commissions, payments of PAYE, national insurance contributions and pension contributions and any other sums due under the Admission Agreement which in any case are attributable in whole or in part to the period from (and including) the Relevant Transfer Date) and any necessary apportionments in respect of any periodic payments shall be made between the Supplier and the Former Supplier.
2. Information
   1. The Supplier shall, and shall procure that each Sub-contractor shall, promptly provide to the Authority and/or at the Authority’s direction, the Former Supplier, in writing such information as is necessary to enable the Authority and/or the Former Supplier to carry out their respective duties under regulation 13 of the Employment Regulations. The Authority shall procure that the Former Supplier shall promptly provide to the Supplier and each Notified Sub-contractor in writing such information as is necessary to enable the Supplier and each Notified Sub-contractor to carry out their respective duties under regulation 13 of the Employment Regulations.
3. Principles of Good Employment Practice
   1. The Supplier shall, and shall procure that each Sub-contractor shall, comply with any requirement notified to it by the Authority relating to pensions in respect of any Transferring Former Supplier Employee as set down in:
      1. the Cabinet Office Statement of Practice on Staff Transfers in the Public Sector of January 2000, revised December 2013;
      2. Old Fair Deal; and/or
      3. the New Fair Deal.
   2. Any changes necessary to this Contract as a result of changes to, or any replacement of any statement of practice, paper or other guidance that replaces any of the documentation referred to in Paragraph 5.1 shall be agreed in accordance with the Change Control Procedure.
4. Procurement Obligations
   1. Notwithstanding any other provisions of this Part B, where in this Part B the Authority accepts an obligation to procure that a Former Supplier does or does not do something, such obligation shall be limited so that it extends only to the extent that the Authority’s contract with the Former Supplier contains a contractual right in that regard which the Authority may enforce, or otherwise so that it requires only that the Authority must use reasonable endeavours to procure that the Former Supplier does or does not act accordingly.
5. Pensions
   1. The Supplier shall, and shall procure that each Sub-contractor shall, comply with:
      1. the requirements of Part 1 of the Pensions Act 2008, section 258 of the Pensions Act 2004 and the Transfer of Employment (Pension Protection) Regulations 2005 for all transferring staff; and
      2. Part D (and its Annexes) to this Staff Transfer Schedule.

## Part C: No Transfer of Employees Expected at Commencement of Services

1. Procedure in the Event of Transfer
   1. The Authority and the Supplier agree that the commencement of the provision of the Services or of any part of the Services is not expected to be a Relevant Transfer in relation to any employees of the Authority and/or any Former Supplier.
   2. If any employee of the Authority and/or a Former Supplier claims, or it is determined in relation to any employee of the Authority and/or a Former Supplier, that his/her contract of employment has been transferred from the Authority and/or the Former Supplier to the Supplier and/or any Sub-contractor pursuant to the Employment Regulations then:
      1. the Supplier shall, and shall procure that the relevant Sub-contractor shall, within 5 Working Days of becoming aware of that fact, give notice in writing to the Authority and, where required by the Authority, give notice to the Former Supplier; and
      2. the Authority and/or the Former Supplier may offer (or may procure that a third party may offer) employment to such person within 15 Working Days of the notification by the Supplier or the Sub-contractor (as appropriate) or take such other reasonable steps as the Authority or Former Supplier (as the case may be) considers appropriate to deal with the matter provided always that such steps are in compliance with applicable Law.
   3. If an offer referred to in Paragraph 1.2.2 is accepted (or if the situation has otherwise been resolved by the Authority and/or the Former Supplier), the Supplier shall, or shall procure that the Sub-contractor shall, immediately release the person from his/her employment or alleged employment.
   4. If by the end of the 15 Working Day period specified in Paragraph 1.2.2:
      1. no such offer of employment has been made;
      2. such offer has been made but not accepted; or
      3. the situation has not otherwise been resolved,

the Supplier and/or the Sub-contractor may within 5 Working Days give notice to terminate the employment or alleged employment of such person.

1. Indemnities
   1. Subject to the Supplier and/or the relevant Sub-contractor acting in accordance with the provisions of Paragraphs 1.2 to 1.4 and in accordance with all applicable employment procedures set out in applicable Law and subject also to Paragraph 2.4, the Authority shall:
      1. indemnify the Supplier and/or the relevant Sub-contractor against all Employee Liabilities arising out of the termination of the employment of any employees of the Authority referred to in Paragraph 1.2 made pursuant to the provisions of Paragraph 1.4 provided that the Supplier takes, or shall procure that the Notified Sub-contractor takes, all reasonable steps to minimise any such Employee Liabilities; and
      2. procure that the Former Supplier indemnifies the Supplier and/or any Notified Sub-contractor against all Employee Liabilities arising out of termination of the employment of the employees of the Former Supplier referred to in Paragraph 1.2 made pursuant to the provisions of Paragraph 1.4 provided that the Supplier takes, or shall procure that the relevant Sub-contractor takes, all reasonable steps to minimise any such Employee Liabilities.
   2. If any such person as is described in Paragraph 1.2 is neither re employed by the Authority and/or the Former Supplier as appropriate nor dismissed by the Supplier and/or any Sub-contractor within the 15 Working Day period referred to in Paragraph 1.4 such person shall be treated as having transferred to the Supplier and/or the Sub-contractor (as appropriate) and the Supplier shall, or shall procure that the Sub-contractor shall, (a) comply with such obligations as may be imposed upon it under Law and (b) comply with the provisions of Part D (*Pensions*) and its Annexes of this Staff Transfer Schedule.
   3. Where any person remains employed by the Supplier and/or any Sub-contractor pursuant to Paragraph 2.2, all Employee Liabilities in relation to such employee shall remain with the Supplier and/or the Sub-contractor and the Supplier shall indemnify the Authority and any Former Supplier, and shall procure that the Sub-contractor shall indemnify the Authority and any Former Supplier, against any Employee Liabilities that either of them may incur in respect of any such employees of the Supplier and/or employees of the Sub-contractor.
   4. The indemnities in Paragraph 2.1:
      1. shall not apply to:
         1. any claim for:

(i) any contravention of the Equality Act 2010 (or predecessor/successor legislation); or

(ii) equal pay or compensation for less favourable treatment of part-time workers or fixed-term employees,

in any case in relation to any alleged act or omission of the Supplier and/or any Sub-contractor; or

* + - 1. any claim that the termination of employment was unfair because the Supplier and/or any Sub-contractor neglected to follow a fair dismissal procedure; and
    1. shall apply only where the notification referred to in Paragraph 1.2.1 is made by the Supplier and/or any Sub-contractor to the Authority and, if applicable, Former Supplier within 6 months of the Relevant Transfer Date.

1. Procurement Obligations
   1. Where in this Part C the Authority accepts an obligation to procure that a Former Supplier does or does not do something, such obligation shall be limited so that it extends only to the extent that the Authority’s contract with the Former Supplier contains a contractual right in that regard which the Authority may enforce, or otherwise so that it requires only that the Authority must use reasonable endeavours to procure that the Former Supplier does or does not act accordingly.

## Part D: Pensions

1. Definitions
   1. In this Part D and Part E, the following words have the following meanings and they shall supplement Schedule 1 (*Definitions*), and shall be deemed to include the definitions set out in the Annexes to this Part D:

|  |  |
| --- | --- |
| “Actuary” | a Fellow of the Institute and Faculty of Actuaries; |
| “Best Value Direction” | the Best Value Authorities Staff Transfers (Pensions) Direction 2007 or the Welsh Authorities Staff Transfers (Pensions) Direction 2012 (as appropriate); |
| “Broadly Comparable” | 1. in respect of a pension scheme, a status satisfying the condition that there are no identifiable employees who will suffer material detriment overall in terms of future accrual of pension benefits as assessed in accordance with Annex A of New Fair Deal and demonstrated by the issue by the Government Actuary’s Department of a broad comparability certificate; and/or 2. in respect of benefits provided for or in respect of a member under a pension scheme, benefits that are consistent with that pension scheme’s certificate of broad comparability issued by the Government Actuary’s Department,   and “Broad Comparability” shall be construed accordingly; |
| “CSPS” | the schemes as defined in Annex D1 to this Part D; |
| “Direction Letter/Determination” | has the meaning in Annex D2 to this Part D; |
| “Fair Deal Eligible Employees” | means each of the CSPS Eligible Employees (as defined in Annex D1 to this Part D), the NHSPS Eligible Employees (as defined in Annex D2 to this Part D) and/or the LGPS Eligible Employees (as defined in Annex D3 to this Part D) (as applicable) (and shall include any such employee who has been admitted to and/or remains eligible to join a Broadly Comparable pension scheme at the relevant time in accordance with Paragraph 10 or 11 of this Part D); |
| “Fair Deal Employees” | any of:   1. Transferring Authority Employees; 2. Transferring Former Supplier Employees; and/or 3. employees who are not Transferring Authority Employees or Transferring Former Supplier Employees but to whom the Employment Regulations apply on the Relevant Transfer Date to transfer their employment to the Supplier or a Sub-Contractor, and whose employment is not terminated in accordance with the provisions of Paragraph 2.5 of Part A or Part B or Paragraph 1.4 of Part C; 4. where the Supplier or a Sub-contractor was the Former Supplier, the employees of the Supplier (or Sub-contractor);   who at the Relevant Transfer Date are or become entitled to New Fair Deal or Best Value Direction protection in respect of any of the Statutory Schemes or a Broadly Comparable pension scheme provided in accordance with Paragraph 10 of this Part D as notified by the Authority; |
| “Fund Actuary” | a Fund Actuary as defined in Annex D3 to this Part D; |
| “LGPS” | the scheme as defined in Annex D3 to this Part D; |
| “NHSPS” | the schemes as defined in Annex D2 to this Part D; and |
| “New Fair Deal” | has the meaning given to it Paragraph 1 (Definitions) of this Schedule. |

1. Participation
   1. In respect of all or any Fair Deal Employees each of Annex D1: CSPS, Annex D2: NHSPS and/or Annex D3: LGPS shall apply, as appropriate.
   2. The Supplier undertakes to do all such things and execute any documents (including any relevant Admission Agreement and/or Direction Letter/Determination, if necessary) as may be required to enable the Supplier to participate in the appropriate Statutory Scheme in respect of the Fair Deal Employees and shall bear its own costs in such regard.
   3. The Supplier undertakes:
      1. to pay to the Statutory Schemes all such amounts as are due under the relevant Admission Agreement and/or Direction Letter/Determination or otherwise and shall deduct and pay to the Statutory Schemes such employee contributions as are required; and
      2. subject to Paragraph 5 of Annex D3: LGPS to be fully responsible for all other costs, contributions, payments and other amounts relating to its participation in the Statutory Schemes, including for the avoidance of doubt any exit payments and the costs of providing any bond, indemnity or guarantee required in relation to such participation.
   4. Where the Supplier is the Former Supplier (or a Sub-contractor is a sub-contractor of the Former Supplier) and there is no Relevant Transfer of the Fair Deal Employees because they remain continuously employed by the Supplier (or Sub-contractor) at the Operational Service Commencement Date, this Part D and its Annexes shall be modified accordingly so that the Supplier (or Sub-contractor) shall comply with its requirements from the Operational Service Commencement Date or, where it previously provided a Broadly Comparable pension scheme, from the date it is able to close accrual of its Broadly Comparable pension scheme (following appropriate consultation and contractual changes as appropriate) if later. The Supplier (or Sub-contractor) shall make arrangements for a bulk transfer from its Broadly Comparable pension scheme to the relevant Statutory Scheme in accordance with the requirements of the previous contract with the Authority.
2. Provision of Information
   1. The Supplier undertakes to the Authority:
      1. to provide all information which the Authority may reasonably request concerning matters referred to in this Part D as expeditiously as possible;
      2. not to issue any announcements to any Fair Deal Employee prior to the Relevant Transfer Date concerning the matters stated in this Part D without the consent in writing of the Authority (such consent not to be unreasonably withheld or delayed); and
      3. retain such records as would be necessary to manage the pension aspects in relation to any current or former Fair Deal Eligible Employees arising on expiry or termination of this Contract.
3. Indemnities
   1. The Supplier shall indemnify and keep indemnified the Authority, [NHS Pensions,] any Replacement Supplier and/or any Replacement Sub-contractor on demand from and against all and any Losses whatsoever suffered or incurred by it or them which:
      1. arise out of or in connection with any liability towards all and any Fair Deal Employees in respect of service on or after the Relevant Transfer Date which arises from any breach by the Supplier of this Part D, and/or the CSPS Admission Agreement and/or the Direction Letter/Determination and/or the LGPS Admission Agreement;
      2. relate to the payment of benefits under and/or participation in a pension scheme (as defined in section 150(1) Finance Act 2004) provided by the Supplier or a Sub-contractor on and after the Relevant Transfer Date until the date of termination or expiry of this Contract, including the Statutory Schemes or any Broadly Comparable pension scheme provided in accordance with Paragraphs 10 or 11 of this Part D;
      3. relate to claims by Fair Deal Employees of the Supplier and/or of any Sub-contractor or by any trade unions, elected employee representatives or staff associations in respect of all or any such Fair Deal Employees which Losses:
         1. relate to any rights to benefits under a pension scheme (as defined in section 150(1) Finance Act 2004) in respect of periods of employment on and after the Relevant Transfer Date until the date of termination or expiry of this Contract;
         2. arise out of the failure of the Supplier and/or any relevant Sub-contractor to comply with the provisions of this Part D before the date of termination or expiry of this Contract; and/or
      4. arise out of or in connection with the Supplier (or its Sub-contractor) allowing anyone who is not an NHSPS Fair Deal Employee to join or claim membership of the NHSPS at any time during the Term.
   2. The indemnities in this Part D and its Annexes:
      1. shall survive termination of this Contract; and
      2. shall not be affected by the caps on liability contained in Clause 23 (*Limitations on Liability*).
4. Disputes
   1. The Dispute Resolution Procedure will not apply to any dispute (i) between the Authority and/or the Supplier or (ii) between their respective actuaries and/or the Fund Actuary about any of the actuarial matters referred to in this Part D and its Annexes shall in the absence of agreement between the Authority and/or the Supplier be referred to an independent Actuary:
      1. who will act as an expert and not as an arbitrator;
      2. whose decision will be final and binding on the Authority and/or the Supplier; and
      3. whose expenses shall be borne equally by the Authority and/or the Supplier unless the independent Actuary shall otherwise direct.
   2. The independent Actuary shall be agreed by the Parties or, failing such agreement the independent Actuary shall be appointed by the President for the time being of the Institute and Faculty of Actuaries on the application by the Parties.
5. Third Party Rights
   1. The Parties agree Clause 41 (*Third Party Rights*) shall apply and that the CRTPA applies to this Part D to the extent necessary to ensure that any Fair Deal Employee will have the right to enforce any obligation in respect of to him or her by the Supplier under this Part D, in his or her or its own right under section 1(1) of the CRTPA.
   2. Further, the Supplier must ensure that the CRTPA will apply to any Sub-contract to the extent necessary to ensure that any Fair Deal Employee will have the right to enforce any obligation owed to them by the Sub-contractor in his or her own right under section 1(1) of the CRTPA.
6. Breach
   1. The Supplier agrees to notify the Authority should it breach any obligations it has under this Part D and agrees that the Authority shall be entitled to terminate its Contract for material Default in the event that the Supplier:
      1. commits an irremediable breach of any provision or obligation it has under this Part D; or
      2. commits a breach of any provision or obligation it has under this Part D which, where capable of remedy, it fails to remedy within a reasonable time and in any event within 28 days of the date of a notice from the Authority giving particulars of the breach and requiring the Supplier to remedy it.
7. Transfer to Another Employer/Sub-contractors
   1. Save on expiry or termination of this Contract, if the employment of any Fair Deal Eligible Employee transfers to another employer (by way of a transfer under the Employment Regulations or other form of compulsory transfer of employment), the Supplier shall or shall procure that any relevant Sub-contractor shall:
      1. notify the Authority as far as reasonably practicable in advance of the transfer to allow the Authority to make the necessary arrangements for participation with the relevant Statutory Scheme(s);
      2. consult with about, and inform those Fair Deal Eligible Employees of, the pension provisions relating to that transfer; and
      3. procure that the employer to which the Fair Deal Eligible Employees are transferred (the “**New Employer**”) complies with the provisions of this Part D and its Annexes provided that references to the “Supplier” will become references to the New Employer, references to “Relevant Transfer Date” will become references to the date of the transfer to the New Employer and references to “Fair Deal Employees” will become references to the Fair Deal Eligible Employees so transferred to the New Employer.
8. Pension Issues on Expiry or Termination
   1. The provisions of Part E: Employment Exit Provisions (Mandatory) apply in relation to pension issues on expiry or termination of this Contract.
   2. The Supplier shall (and shall procure that any of its Sub-contractors shall) prior to the termination of this Contract provide all such co-operation and assistance (including co-operation and assistance from the Broadly Comparable pension scheme’s Actuary) as the Replacement Supplier and/or NHS Pension and/or CSPS and/or the relevant Administering Authority and/or the Authority may reasonably require, to enable the Replacement Supplier to participate in the appropriate Statutory Scheme in respect of any Fair Deal Eligible Employee that remains eligible for New Fair Deal protection following a Service Transfer.
9. Broadly Comparable Pension Scheme on Relevant Transfer Date
   1. If the terms of any of Paragraphs 4 of Annex D2: NHSPS or 3.1 of Annex D3: LGPS applies, the Supplier must (and must, where relevant, procure that each of its Sub-contractors will) ensure that, with effect from the Relevant Transfer Date until the day before the Service Transfer Date, the relevant Fair Deal Employees will be eligible for membership of a pension scheme under which the benefits are Broadly Comparable to those provided under the relevant Statutory Scheme, and then on such terms as may be decided by the Authority.
   2. Such Broadly Comparable pension scheme must be:
      1. established by the Relevant Transfer Date;
      2. a registered pension scheme for the purposes of Part 4 of the Finance Act 2004;
      3. capable of receiving a bulk transfer payment from the relevant Statutory Scheme or from a Former Supplier’s Broadly Comparable pension scheme (unless otherwise instructed by the Authority);
      4. capable of paying a bulk transfer payment to the Replacement Supplier’s Broadly Comparable pension scheme (or the relevant Statutory Scheme if applicable) (unless otherwise instructed by the Authority); and
      5. maintained until such bulk transfer payments have been received or paid (unless otherwise instructed by the Authority).
   3. Where the Supplier has provided a Broadly Comparable pension scheme pursuant to the provisions of this Paragraph 10, the Supplier shall (and shall procure that any of its Sub-contractors shall):
      1. supply to the Authority details of its (or its Sub-contractor’s) Broadly Comparable pension scheme and provide a full copy of the valid certificate of broad comparability (which remains valid as at the Relevant Transfer Date) covering all relevant Fair Deal Employees, as soon as it is able to do so before the Relevant Transfer Date (where possible) and in any event no later than seven (7) days after receipt of the certificate;
      2. be fully responsible for all costs, contributions, payments and other amounts relating to the setting up, certification of, ongoing participation in and/or withdrawal and exit from the Broadly Comparable pension scheme, including for the avoidance of doubt any debts arising under section 75 or 75A of the Pensions Act 1995;
      3. instruct any such Broadly Comparable pension scheme’s Actuary to provide all such co-operation and assistance in agreeing bulk transfer process with the Actuary to the Former Supplier’s Broadly Comparable pension scheme or the Actuary to the relevant Statutory Scheme (as appropriate) and to provide all such co-operation and assistance with any other Actuary appointed by the Authority (where applicable). This will be with a view to the bulk transfer terms providing day for day and/or pound for pound (as applicable) (or actuarially equivalent where there are benefit differences between the two schemes) credits in the Broadly Comparable pension scheme in respect of any Fair Deal Eligible Employee who consents to such a transfer; and
      4. provide a replacement Broadly Comparable pension scheme in accordance with this Paragraph 10 with immediate effect for those Fair Deal Eligible Employees who are still employed by the Supplier and/or relevant Sub-contractor and are still eligible for New Fair Deal protection in the event that the Supplier and/or Sub-contractor’s Broadly Comparable pension scheme is closed to future accrual and/or terminated. The relevant Fair Deal Eligible Employees must be given the option to transfer their accrued benefits from the previous Broadly Comparable pension scheme to the new Broadly Comparable pension scheme on day for day and/or pound for pound terms (as applicable) (or actuarially equivalent where there are benefit differences between the two schemes).
   4. Where the Supplier has provided a Broadly Comparable pension scheme pursuant to the provisions of this Paragraph 10, the Supplier shall (and shall procure that any of its Sub-contractors shall) prior to the termination of this Contract:
      1. allow and make all necessary arrangements to effect, in respect of any Fair Deal Eligible Employee that remains eligible for New Fair Deal protection, following a Service Transfer, the bulk transfer of past service from any such Broadly Comparable pension scheme into the Replacement Supplier’s Broadly Comparable pension scheme (or the relevant Statutory Scheme if applicable). The bulk transfer terms provided shall be on a past service reserve basis which should be calculated allowing for projected final salary at the assumed date of retirement, leaving service or death (in the case of final salary benefits). The actuarial basis for this past service reserve basis should be aligned to the funding requirements of the Broadly Comparable pension scheme in place at the time the bulk transfer terms are offered. The bulk transfer terms shall be subject to an underpin in relation to any service credits awarded in the Broadly Comparable pension scheme in accordance with Paragraph 10.3.3 such that the element of the past service reserve amount which relates to such service credits shall be no lower than that required by the bulk transfer terms that were agreed in accordance with Paragraph 10.3.3 but using the last day of the Fair Deal Eligible Employees’ employment with the Supplier or Sub-contractor (as appropriate) as the date used to determine the actuarial assumptions; and
      2. if the transfer payment paid by the trustees of the Broadly Comparable pension scheme is less (in the opinion of the Actuary to the Replacement Supplier’s Broadly Comparable pension scheme (or to the relevant Statutory Scheme if applicable)) than the transfer payment which would have been paid had Paragraph 10.4.1 been complied with, the Supplier shall (or shall procure that the Sub-contractor shall) pay the amount of the difference to the Replacement Supplier’s Broadly Comparable pension scheme (or relevant Statutory Scheme if applicable) or as the Authority shall otherwise direct. The Supplier shall indemnify the Authority or the Replacement Supplier’s Broadly Comparable pension scheme (or the relevant Statutory Scheme if applicable) (as the Authority directs) for any failure to pay the difference as required under this Paragraph.
10. Broadly Comparable Pension Scheme in Other Circumstances
    1. If the terms of any of Paragraphs 2.2 of Annex D1: CSPS, 5.2 of Annex D2: NHSPS and/or 3.2 of Annex D3: LGPS apply, the Supplier must (and must, where relevant, procure that each of its Sub-contractors will) ensure that, with effect from the cessation of participation in the Statutory Scheme, until the day before the Service Transfer Date, the relevant Fair Deal Eligible Employees will be eligible for membership of a pension scheme under which the benefits are Broadly Comparable to those provided under the relevant Statutory Scheme at the date of cessation of participation in the relevant Statutory Scheme, and then on such terms as may be decided by the Authority.
    2. Such Broadly Comparable pension scheme must be:
       1. established by the date of cessation of participation in the Statutory Scheme;
       2. a registered pension scheme for the purposes of Part 4 of the Finance Act 2004;
       3. capable of receiving a bulk transfer payment from the relevant Statutory Scheme (where instructed to do so by the Authority);
       4. capable of paying a bulk transfer payment to the Replacement Supplier’s Broadly Comparable pension scheme (or the relevant Statutory Scheme if applicable) (unless otherwise instructed by the Authority); and
       5. maintained until such bulk transfer payments have been received or paid (unless otherwise instructed by the Authority).
    3. Where the Supplier has provided a Broadly Comparable pension scheme pursuant to the provisions of this Paragraph 11, the Supplier shall (and shall procure that any of its Sub-contractors shall):
       1. supply to the Authority details of its (or its Sub-contractor’s) Broadly Comparable pension scheme and provide a full copy of the valid certificate of broad comparability (which remains valid as at the date of cessation of participation in the Statutory Scheme) covering all relevant Fair Deal Eligible Employees, as soon as it is able to do so before the cessation of participation in the Statutory Scheme (where possible) and in any event no later than seven (7) days after receipt of the certificate;
       2. be fully responsible for all costs, contributions, payments and other amounts relating to the setting up, certification of, ongoing participation in and/or withdrawal and exit from the Broadly Comparable pension scheme, including for the avoidance of doubt any debts arising under section 75 or 75A of the Pensions Act 1995; and
       3. where required to do so by the Authority, instruct any such Broadly Comparable pension scheme’s Actuary to provide all such co-operation and assistance in agreeing a bulk transfer process with the Actuary to the relevant Statutory Scheme and to provide all such co-operation and assistance with any other Actuary appointed by the Authority (where applicable). The Supplier must ensure that day for day and/or pound for pound (as applicable) (or actuarially equivalent where there are benefit differences between the two schemes) credits in the Broadly Comparable pension scheme are provided in respect of any Fair Deal Employee who consents to such a transfer from the Statutory Scheme and the Supplier shall be fully responsible for any costs of providing those credits in excess of the bulk transfer payment received by the Broadly Comparable pension scheme; and
       4. provide a replacement Broadly Comparable pension scheme in accordance with this Paragraph 11 with immediate effect for those Fair Deal Eligible Employees who are still employed by the Supplier and/or relevant Sub-contractor and are still eligible for New Fair Deal protection in the event that the Supplier and/or Sub-contractor’s Broadly Comparable pension scheme is closed to future accrual and/or terminated. The relevant Fair Deal Eligible Employees must be given the option to transfer their accrued benefits from the previous Broadly Comparable pension scheme to the new Broadly Comparable pension scheme on day for day and/or pound for pound terms (as applicable) (or actuarially equivalent where there are benefit differences between the two schemes).
    4. Where the Supplier has provided a Broadly Comparable pension scheme pursuant to the provisions of this Paragraph 11, the Supplier shall (and shall procure that any of its Sub-contractors shall) prior to the termination of this Contract allow and make all necessary arrangements to effect, in respect of any Fair Deal Eligible Employee that remains eligible for New Fair Deal protection, following a Service Transfer, the bulk transfer of past service from any such Broadly Comparable pension scheme into the Replacement Supplier’s Broadly Comparable pension scheme (or relevant Statutory Scheme if applicable). The bulk transfer terms provided shall be sufficient to secure day for day and/or pound for pound credits (as applicable) (or actuarially equivalent where there are benefit differences between the two schemes) in the Replacement Supplier’s Broadly Comparable pension scheme (or relevant Statutory Scheme if applicable). For the avoidance of doubt, should the amount offered by the Broadly Comparable pension scheme be less than the amount required by the Replacement Supplier’s Broadly Comparable pension scheme (or the relevant Statutory Scheme if applicable) to fund the required credits (“the Shortfall”), the Supplier or the Sub-contractor (as agreed between them) must pay the Replacement Supplier’s Broadly Comparable pension scheme (or relevant Statutory Scheme if applicable) the Shortfall as required, provided that in the absence of any agreement between the Supplier and any Sub-contractor, the Shortfall shall be paid by the Supplier. The Supplier shall indemnify the Authority or the Replacement Supplier’s Broadly Comparable pension scheme (or the relevant Statutory Scheme if applicable) (as the Authority directs) for any failure to pay the Shortfall under this Paragraph.
11. Right of Set-Off
    1. The Authority shall have a right to set off against any payments due to the Supplier under this Contract an amount equal to:
       1. any unpaid employer’s contributions or employee’s contributions or any other financial obligations under the CSPS or any CSPS Admission Agreement in respect of the CSPS Eligible Employees whether due from the Supplier or from any relevant Sub-contractor or due from any third party under any indemnity, bond or guarantee;
       2. any unpaid employer’s contributions or employee’s contributions or any other financial obligations under the NHSPS or any Direction Letter/Determination in respect of the NHSPS Eligible Employees whether due from the Supplier or from any relevant Sub-contractor or due from any third party under any indemnity, bond or guarantee; or
       3. any unpaid employer’s contributions or employee’s contributions or any other financial obligations under the LGPS or any LGPS Admission Agreement in respect of the LGPS Eligible Employees whether due from the Supplier or from any relevant Sub-contractor or due from any third party under any indemnity, bond or guarantee;

and shall pay such set off amount to the relevant Statutory Scheme.

* 1. The Authority shall also have a right to set off against any payments due to the Supplier under this Contract all reasonable costs and expenses incurred by the Authority as result of Paragraphs 12.1 above.

## Annex D1: CSPS

1. Definitions
   1. In this Annex D1: CSPS to Part D: Pensions, the following words have the following meanings:

|  |  |
| --- | --- |
| “CSPS Admission Agreement” | an admission agreement in the form available on the Civil Service Pensions website immediately prior to the Relevant Transfer Date to be entered into for the CSPS in respect of the Services; |
| “CSPS Eligible Employee” | any CSPS Fair Deal Employee who at the relevant time is an active member or eligible to participate in the CSPS under a CSPS Admission Agreement; |
| “CSPS Fair Deal Employee” | a Fair Deal Employee who at the Relevant Transfer Date is or becomes entitled to protection in respect of the CSPS in accordance with the provisions of New Fair Deal; and |
| “CSPS” | the "Alpha" pension scheme introduced under The Public Service (Civil Servants and Others) Pensions Regulations 2014 available to Civil Servants and employees of bodies under Schedule 1 of the Superannuation Act 1972 (and eligible employees of other bodies admitted to participate under a determination under section 25 of the Public Service Pensions Act 2013), as governed by rules adopted by Parliament; the Partnership Pension Account and its (i) Ill health Benefits Arrangements and (ii) Death Benefits Arrangements; the Civil Service Additional Voluntary Contribution Scheme. |

1. Future Service Benefits
   1. In accordance with New Fair Deal, the Supplier and/or any of its Sub-contractors to which the employment of any CSPS Fair Deal Employee compulsorily transfers as a result of either the award of this Contract or a Relevant Transfer, if not an employer which participates automatically in the CSPS, shall each secure a CSPS Admission Agreement to ensure that CSPS Fair Deal Employees or CSPS Eligible Employees as appropriate shall be either admitted into, or offered continued membership of, the relevant section of the CSPS that they currently contribute to, or were eligible to join immediately prior to the Relevant Transfer Date or became eligible to join on the Relevant Transfer Date. The Supplier and/or any of its Sub-contractors shall procure that the CSPS Fair Deal Employees continue to accrue benefits in the CSPS in accordance with the provisions governing the relevant section of the CSPS for service from (and including) the Relevant Transfer Date.
   2. If the Supplier and/or any of its Sub-contractors enters into a CSPS Admission Agreement in accordance with Paragraph 2.1 but the CSPS Admission Agreement is terminated during the term of this Contract for any reason at a time when the Supplier or Sub-contractor still employs any CSPS Eligible Employees, the Supplier shall (and procure that its Sub-contractors shall) at no extra cost to the Authority, offer the remaining CSPS Eligible Employees membership of a pension scheme which is Broadly Comparable to the CSPS on the date those CSPS Eligible Employees ceased to participate in the CSPS in accordance with the provisions of Paragraph 11 of Part D.

## Annex D2: NHSPS

1. Definitions
   1. In this Annex D2: NHSPS to Part D: Pensions, the following words have the following meanings:

|  |  |
| --- | --- |
| “Direction Letter/Determination” | an NHS Pensions Direction or Determination (as appropriate) issued by the Secretary of State in exercise of the powers conferred by section 7 of the Superannuation (Miscellaneous Provisions) Act 1967 or by section 25 of the Public Service Pensions Act 2013 (as appropriate) and issued to the Supplier or a Sub-contractor of the Supplier (as appropriate) relating to the terms of participation of the Supplier or Sub-contractor in the NHSPS in respect of the NHSPS Fair Deal Employees; |
| “NHS Broadly Comparable Employees” | means each of the Fair Deal Employees who at a Relevant Transfer Date was a member of, or was entitled to become a member of, or but for their compulsory transfer of employment would have been entitled to be or become a member of, the NHSPS as a result of either:   1. their employment with the Authority, an NHS Body or other employer which participates automatically in the NHSPS; or 2. their employment with a Former Supplier who provides access to either the NHSPS pursuant to a Direction Letter/Determination or to a Broadly Comparable pension scheme in respect of their employment with that Former Supplier (on the basis that they are entitled to protection under New Fair Deal (or previous guidance), having been formerly in employment with the Authority, an NHS Body or other employer who participated automatically in the NHSPS in connection with the Services, prior to being employed by the Former Supplier),   but who is now ineligible to participate in the NHSPS under the rules of the NHSPS and in respect of whom the Authority has agreed are to be provided with a Broadly Comparable pension scheme to provide Pension Benefits that are Broadly Comparable to those provided under the NHSPS. |
| “NHSPS Eligible Employees” | any NHSPS Fair Deal Employee who at the relevant time is an active member or eligible to participate in the NHSPS under a Direction Letter/Determination Letter. |
| “NHSPS Fair Deal Employees” | means other than the NHS Broadly Comparable Employees, each of the Fair Deal Employees who at a Relevant Transfer Date was a member of, or was entitled to become a member of, or but for their compulsory transfer of employment would have been entitled to be or become a member of, the NHSPS as a result of either:   1. their employment with the Authority, an NHS Body or other employer which participates automatically in the NHSPS; or 2. their employment with a Former Supplier who provides access to either the NHSPS pursuant to a Direction Letter/Determination or to a Broadly Comparable pension scheme in respect of their employment with that Former Supplier (on the basis that they are entitled to protection under New Fair Deal (or previous guidance), having been formerly in employment with the Authority, an NHS Body or other employer who participated automatically in the NHSPS in connection with the Services, prior to being employed by the Former Supplier),   and, in each case, being continuously engaged for more than fifty per cent (50%) of their employed time in the delivery of services (the same as or similar to the Services).  For the avoidance of doubt, an individual who is in or entitled to become a member of the NHSPS as a result of being engaged in the Services and being covered by an “open” Direction Letter/Determination or other NHSPS “access” facility but who has never been employed directly by the Authority, an NHS Body or other body which participates automatically in the NHSPS is not an NHSPS Fair Deal Employee; |
| “NHS Body” | has the meaning given to it in section 275 of the National Health Service Act 2006 as amended by section 138(2)(c) of Schedule 4 to the Health and Social Care Act 2012; |
| “NHS Pensions” | NHS Pensions as the administrators of the NHSPS or such other body as may from time to time be responsible for relevant administrative functions of the NHSPS; |
| “NHSPS” | the National Health Service Pension Scheme for England and Wales, established pursuant to the Superannuation Act 1972 and the Public Service Pensions Act 2013 governed by subsequent regulations under those Acts including the NHS Pension Scheme Regulations; |
| “NHS Pension Scheme Regulations” | as appropriate, any or all of the National Health Service Pension Scheme Regulations 1995 (SI 1995/300), the National Health Service Pension Scheme Regulations 2008 (SI 2008/653), the National Health Service Pension Scheme Regulations 2015 (2015/94) and any subsequent regulations made in respect of the NHSPS, each as amended from time to time; |
| “NHS Premature Retirement Rights” | rights to which any NHSPS Fair Deal Employee (had they remained in the employment of the Authority, an NHS Body or other employer which participates automatically in the NHSPS) would have been or is entitled under the NHS Pension Scheme Regulations, the NHS Compensation for Premature Retirement Regulations 2002 (SI 2002/1311), the NHS (Injury Benefits) Regulations 1995 (SI 1995/866) and section 45 of the General Whitley Council conditions of service, or any other legislative or contractual provision which replaces, amends, extends or consolidates the same from time to time; and |
| “Pension Benefits” | any benefits payable in respect of an individual (including but not limited to pensions related allowances and lump sums) relating to old age, invalidity or survivor’s benefits provided under an occupational pension scheme. |

1. Membership of the NHSPS
   1. In accordance with New Fair Deal, the Supplier and/or any of its Sub-contractors to which the employment of any NHSPS Fair Deal Employee compulsorily transfers as a result of either the award of this Contract or a Relevant Transfer, if not an NHS Body or other employer which participates automatically in the NHSPS, shall each secure a Direction Letter/Determination to enable the NHSPS Fair Deal Employees to retain either continuous active membership of or eligibility for the NHSPS for so long as they remain employed in connection with the delivery of the Services under this Contract.
   2. Where it is not possible for the Supplier and/or any of its Sub-contractors to secure a Direction Letter/Determination on or before the Relevant Transfer Date, the Supplier must secure a Direction Letter/Determination as soon as possible after the Relevant Transfer Date, and in the period between the Relevant Transfer Date and the date the Direction Letter/Determination is secure, the Provider must ensure that:
      1. all employer’s and NHSPS Fair Deal Employees’ contributions intended to go to the NHSPS are kept in a separate bank account; and
      2. the Pension Benefits and Premature Retirement Rights of NHSPS Fair Deal Employees are not adversely affected.
   3. The Supplier must supply to the Authority a complete copy of each Direction Letter/Determination within 5 Working Days of receipt of the Direction Letter/Determination.
   4. The Supplier must ensure (and procure that each of its Sub-contractors (if any) ensures) that all of its NHSPS Fair Deal Employees have a contractual right to continuous active membership of or eligibility for the NHSPS for so long as they have a right to membership or eligibility of that scheme under the terms of the Direction Letter/Determination.
   5. The Supplier will (and will procure that its Sub-contractors (if any) will) comply with the terms of the Direction Letter/Determination, the NHS Pension Scheme Regulations (including any terms which change as a result of changes in Law) and any relevant policy issued by the Department of Health and Social Care in respect of the NHSPS Fair Deal Employees for so long as it remains bound by the terms of any such Direction Letter/Determination.
   6. Where any employee omitted from the Direction Letter/Determination supplied in accordance with Paragraph 2 of this Annex are subsequently found to be an NHSPS Fair Deal Employee, the Supplier will (and will procure that its Sub-contractors (if any) will) treat that person as if they had been an NHSPS Fair Deal Employee from the Relevant Transfer Date so that their Pension Benefits and NHS Premature Retirement Rights are not adversely affected.
   7. The Supplier will (and will procure that its Sub-contractors (if any) will) provide any indemnity, bond or guarantee required by NHS Pensions in relation to a Direction Letter/Determination.
2. NHS Premature Retirement Rights
   1. From the Relevant Transfer Date until the Service Transfer Date, the Supplier must provide (and/or must ensure that its Sub-contractors (if any) provide) NHS Premature Retirement Rights in respect of the NHSPS Fair Deal Employees that are identical to the benefits they would have received had they remained employees of the Authority, an NHS Body or other employer which participates automatically in the NHSPS.
3. NHS Broadly Comparable Employees
   1. The Supplier shall (and procure that its Sub-contractors shall), with effect from the Relevant Transfer Date, offer the NHSPS Broadly Comparable Employees membership of a pension scheme which is Broadly Comparable to NHSPS on the Relevant Transfer Date in accordance with Paragraph 10 of Part D. For the avoidance of doubt, this requirement is separate from any requirement to offer a Broadly Comparable pension scheme in accordance with Paragraph 5.2 below.
4. Breach and Cancellation of any Direction Letter/Determination(s)
   1. The Supplier agrees that the Authority is entitled to make arrangements with NHS Pensions for the Authority to be notified if the Supplier (or its Sub-contractors) breaches the terms of its Direction Letter/Determination. Notwithstanding the provisions of the foregoing, the Supplier shall notify the Authority in the event that it (or its Sub-contractor) breaches the terms of its Direction Letter/Determination.
   2. If the Supplier (or its Sub-contractors, if relevant) ceases to participate in the NHSPS for whatever reason, the Supplier (or any such Sub-contractor, as appropriate) shall offer the NHSPS Eligible Employees membership of a pension scheme which is Broadly Comparable to the NHSPS on the date the NHSPS Eligible Employees ceased to participate in the NHSPS in accordance with the provisions of Paragraph 11 of Part D.
5. Compensation
   1. If the Supplier (or its Sub-contractor, if relevant) is unable to provide the NHSPS Fair Deal Employees with either membership of:
      1. the NHSPS (having used its best endeavours to secure a Direction Letter/Determination); or
      2. a Broadly Comparable pension scheme,

the Authority may in its sole discretion permit the Supplier (or any of its Sub-contractors) to compensate the NHSPS Fair Deal Employees in a manner that is Broadly Comparable or equivalent in cash terms, the Supplier (or Sub-contractor as relevant) having consulted with a view to reaching agreement with any recognised trade union or, in the absence of such body, the NHSPS Fair Deal Employees. The Supplier must meet (or must procure that the relevant Sub-contractor meets) the costs of the Authority determining whether the level of compensation offered is reasonable in the circumstances.

* 1. This flexibility for the Authority to allow compensation in place of Pension Benefits is in addition to and not instead of the Authority’s right to terminate the Contract under Paragraph 7 (*Breach*) of Part D of this Schedule.

1. Supplier Indemnities
   1. The Supplier must indemnify and keep indemnified the Authority and any Replacement Supplier against all Losses arising out of any claim by any NHSPS Fair Deal Employee or any NHS Broadly Comparable Employees that the provision of (or failure to provide) Pension Benefits and NHS Premature Retirement Rights from the Relevant Transfer Date, or the level of such benefit provided, constitutes a breach of his or her employment rights.

## Annex D3: LGPS

1. Definitions
   1. In this Annex D3 LGPS to Part D: Pensions, the following words have the following meanings:

|  |  |
| --- | --- |
| “2013 Regulations” | the Local Government Pension Scheme Regulations 2013 (SI 2013/2356) (as amended from time to time); |
| “Administering Authority” | in relation to the Fund [insert name], the relevant administering authority of that Fund for the purposes of the 2013 Regulations; |
| “Fund Actuary” | the actuary to a Fund appointed by the Administering Authority of the Fund; |
| “Fund” | [insert name], a pension fund within the LGPS; |
| [“Initial Contribution Rate”] | [XX**%**] of pensionable pay (as defined in the 2013 Regulations);] |
| “LGPS” | the Local Government Pension Scheme as governed by the LGPS Regulations, and any other regulations (in each case as amended from time to time) which are from time to time applicable to the Local Government Pension Scheme; |
| “LGPS Admission Agreement” | an admission agreement within the meaning in Schedule 1 of the 2013 Regulations; |
| “LGPS Admission Body” | an admission body (within the meaning of Part 3 of Schedule 2 of the 2013 Regulations); |
| “LGPS Eligible Employees” | any LGPS Fair Deal Employee who at the relevant time is an active member or eligible to participate in the LGPS under an LGPS Admission Agreement; |
| “LGPS Fair Deal Employees” | any Fair Deal Employee who at the Relevant Transfer Date is or becomes entitled to protection in respect of the LGPS or a pension scheme that is Broadly Comparable to the LGPS in accordance with the provisions in accordance with the provisions of New Fair Deal and/or the Best Value Direction; and |
| “LGPS Regulations” | the 2013 Regulations and The Local Government Pension Scheme (Transitional Provisions, Savings and Amendment) Regulations 2014 (SI 2014/525), and any other regulations (in each case as amended from time to time) which are from time to time applicable to the LGPS. |

1. Supplier to Become an LGPS Admission Body
   1. In accordance with the principles of New Fair Deal and/or the Best Value Direction, the Supplier and/or any of its Sub-contractors to which the employment of any LGPS Fair Deal Employee compulsorily transfers as a result of either the award of this Contract or a Relevant Transfer, if not a scheme employer which participates automatically in the LGPS, shall each become an LGPS Admission Body by entering into an LGPS Admission Agreement with effect from the Relevant Transfer Date to enable the LGPS Fair Deal Employees to retain either continuous active membership of or eligibility for the LGPS on and from the Relevant Transfer Date for so long as they remain employed in connection with the delivery of the Services under this Contract.

OPTION 1

* 1. [Any LGPS Fair Deal Employees who:
     1. were active members of the LGPS (or a Broadly Comparable pension scheme) immediately before the Relevant Transfer Date shall be admitted to the LGPS with effect on and from the Relevant Transfer Date; and
     2. were eligible to join the LGPS (or a Broadly Comparable pension scheme) but were not active members of the LGPS (or a Broadly Comparable pension scheme) immediately before the Relevant Transfer Date shall retain the ability to join the LGPS on or after the Relevant Transfer Date if they wish to do so.]

OPTION 2

[Any LGPS Fair Deal Employees whether:

* + 1. active members of the LGPS (or a Broadly Comparable pension scheme) immediately before the Relevant Transfer Date; or
    2. eligible to join the LGPS (or a Broadly Comparable pension scheme) but not active members of the LGPS (or a Broadly Comparable pension scheme) immediately before the Relevant Transfer Date

shall be admitted to the LGPS with effect on and from the Relevant Transfer Date. The Supplier shall not automatically enrol or re-enrol for the purposes of the Pensions Act 2008 any LGPS Fair Deal Employees in any pension scheme other than the LGPS unless they cease to be eligible for membership of the LGPS.]

* 1. The Supplier will (and will procure that its Sub-contractors (if any) will) provide at its own cost any indemnity, bond or guarantee required by an Administering Authority in relation to an LGPS Admission Agreement.

1. Broadly Comparable Scheme
   1. If the Supplier and/or any of its Sub-contractors is unable to obtain an LGPS Admission Agreement in accordance with Paragraph 2.1 because the Administering Authority will not allow it to participate in the Fund, the Supplier shall (and procure that its Sub-contractors shall), with effect from the Relevant Transfer Date, offer the LGPS Fair Deal Employees membership of a pension scheme which is Broadly Comparable to LGPS on the Relevant Transfer Date in accordance with the provisions of Paragraph 10 of Part D.
   2. If the Supplier and/or any of its Sub-contractors becomes an LGPS Admission Body in accordance with Paragraph 2.1 but the LGPS Admission Agreement is terminated during the term of this Contract for any reason at a time when the Supplier or Sub-contractors still employs any LGPS Eligible Employees, the Supplier shall (and procure that its Sub-contractors shall) at no extra cost to the Authority, offer the remaining LGPS Eligible Employees membership of a pension scheme which is Broadly Comparable to the LGPS on the date the LGPS Eligible Employees ceased to participate in the LGPS in accordance with the provisions of Paragraph 11 of Part D.
2. Discretionary Benefits
   1. Where the Supplier and/or any of its Sub-contractors is an LGPS Admission Body, the Supplier shall (and procure that its Sub-contractors shall) comply with its obligations under regulation 60 of the 2013 Regulations in relation to the preparation of a discretionary policy statement.
3. LGPS Risk Sharing
   1. Subject to Paragraphs 5.4 to 5.10, if at any time during the term of this Contract the Administering Authority, pursuant to the LGPS Admission Agreement or the LGPS Regulations, requires the Supplier or any Sub-contractor to pay employer contributions or other payments to the Fund in aggregate in excess of the Initial Contribution Rate, the excess of employer contributions above the Initial Contribution Rate for a Contract Year (the “Excess Amount”) shall be paid by the Supplier or the Sub-contractor, as the case may be, and the Supplier shall be reimbursed by the Authority.
   2. Subject to Paragraphs 5.4 to 5.9 and 5.11, if at any time during the term of this Contract, the Administering Authority, pursuant to the LGPS Admission Agreement or the LGPS Regulations, requires the Supplier or any Sub-contractor to pay employer contributions or payments to the Fund in aggregate below the Initial Contribution Rate for a Contract Year, the Supplier shall reimburse the Authority an amount equal to A–B (the “Refund Amount”) where:

A = the amount which would have been paid if contributions and payments had been paid equal to the Initial Contribution Rate for that Contract Year; and

B = the amount of contributions or payments actually paid by the Supplier or Sub-contractor for that Contract Year, as the case may be, to the Fund.

* 1. Subject to Paragraphs 5.4 to 5.10, where the Administering Authority obtains an actuarial valuation and a revised rates and adjustment certificate under the LGPS Regulations and/or the terms of the LGPS Admission Agreement when the LGPS Admission Agreement ceases to have effect and the Supplier or any Sub-contractor is required to pay any exit payment under Regulation 64(2) of the 2013 Regulations (the “Exit Payment”), such Exit Payment shall be paid by the Supplier or any Sub-contractor (as the case may be) and the Supplier shall be reimbursed by the Authority.
  2. The Supplier and any Sub-contractors shall at all times be responsible for the following costs:
     1. any employer contributions relating to the costs of early retirement benefits arising on redundancy or as a result of business efficiency under Regulation 30(7) of the 2013 Regulations or otherwise;
     2. any payment of Fund benefits to active members on the grounds of ill health or infirmity of mind or body under Regulation 35 of the 2013 Regulations or otherwise;
     3. any payment of Fund benefits to deferred or deferred pensioner members on the grounds of ill health or infirmity of mind or body under Regulation 38 of the 2013 Regulations or otherwise;
     4. any employer contributions relating to the costs of early or flexible retirement where the actuarial reduction is waived in whole or in part or a cost neutral reduction is not applied with the consent of the Supplier or any relevant Sub-contractor including without limitation any decision made under Regulation 30(8) of the 2013 Regulations or Schedule 2 of The Local Government Pension Scheme (Transitional Provisions, Savings and Amendment) Regulations 2014;
     5. any employer contributions relating to the costs of enhanced benefits made at the discretion of the Supplier or any relevant Sub-contractors including without limitation additional pension awarded under Regulation 31 of the 2013 Regulations or otherwise;
     6. any increase to the employer contribution rate resulting from the award of pay increases by the Supplier or relevant Sub-contractors in respect of all or any of the LGPS Eligible Employees in excess of the pay increases assumed in the Fund’s most recent actuarial valuation (unless the Supplier and/or any Sub-contractor is contractually bound to provide such increases on the Relevant Transfer Date);
     7. to the extent not covered above, any other costs arising out of or in connection with the exercise of any discretion or the grant of any consent under the LGPS Regulations by the Supplier or any relevant Sub-contractors where a member does not have an absolute entitlement to that benefit under the LGPS;
     8. any cost of the administration of the Fund that are not met through the Supplier’s or Sub-contractor’s employer contribution rate, including without limitation an amount specified in a notice given by the Administering Authority under Regulation 70 of the 2013 Regulations;
     9. the costs of any reports and advice requested by or arising from an instruction given by the Supplier or a Sub-contractor from the Fund Actuary; and/or
     10. any interest payable under the 2013 Regulations or LGPS Administration Agreement.
  3. For the purposes of calculating any Exit Payment, Excess Amount or Refund Amount, any part of such an amount which is attributable to any costs which the Supplier or Sub-contractors are responsible for in accordance with Paragraph 5.4 above shall be disregarded and excluded from the calculation. In the event of any dispute as to level of any cost that should be excluded from the calculation, the opinion of the Fund Actuary shall be final and binding.
  4. Where the Administering Authority obtains an actuarial valuation and a revised rates and adjustment certificate under the LGPS Regulations and/or the terms of the LGPS Admission Agreement when the LGPS Admission Agreement ceases to have effect and the Supplier or any Sub-contractor receives payment of an exit credit payment under Regulation 64(2) of the 2013 Regulations (the “Exit Credit”), the Supplier shall (or procure that any Sub-contractor shall) reimburse the Authority an amount equal to the Exit Credit within twenty (20) Working Days of receipt of the Exit Credit.
  5. The Supplier shall (or procure that the Sub-contractor shall) notify the Authority in writing within twenty (20) Working Days:
     1. of the end of each Contract Year of any Excess Amount or Refund Amount due in respect of the Contract Year that has just ended and provide a reasonable summary of how the Excess Amount or Refund Amount was calculated; and
     2. of being informed by the Administering Authority of any Exit Payment or Exit Credit that is determined by as being due from or to the Supplier or a Sub-contractor and provide a copy of any revised rates and adjustments certificate detailing the Exit Payment or Exit Credit and its calculation.
  6. Within twenty (20) Working Days of receiving the notification under Paragraph 5.7 above, the Authority shall either:
     1. notify the Supplier in writing of its acceptance of the Excess Amount, Refund Amount or Exit Payment;
     2. request further information or evidence about the Excess Amount, Refund Amount or Exit Payment from the Supplier; and/or
     3. request a meeting with the Supplier to discuss or clarify the information or evidence provided.
  7. Where the Excess Amount, Refund Amount or Exit Payment is agreed following the receipt of further information or evidence or following a meeting in accordance with Paragraph 5.8 above, the Authority shall notify the Supplier in writing. In the event that the Supplier and the Authority are unable to agree the amount of the Excess Amount, Refund Amount or Exit Payment then they shall follow the Dispute Resolution Procedure.
  8. Any Excess Amount or Exit Payment agreed by the Authority or in accordance with the Dispute Resolution Procedure shall be paid by the Authority within timescales as agreed between Authority and Supplier. The amount to be paid by the Authority shall be an amount equal to the Excess Amount or Exit Payment less an amount equal to any corporation tax relief which has been claimed in respect of the Excess Amount or Exit Payment by the Supplier or a Sub-contractor.
  9. Any Refund Amount agreed by the Authority or in accordance with the Dispute Resolution Procedure as payable by the Supplier or any Sub-contractor to the Authority, shall be paid by the Supplier or any Sub-contractor forthwith as the liability has been agreed. In the event the Supplier or any Sub-contractor fails to pay any agreed Refund Amount, the Authority shall demand in writing the immediate payment of the agreed Refund Amount by the Supplier and the Supplier shall make payment within seven (7) Working Days of such demand.
  10. This Paragraph 5 shall survive termination of this Contract.

## Annex D4: Other Schemes

***[Guidance: Placeholder for Pension Schemes other than LGPS, CSPS & NHSPS]***

## Part E: Employment Exit Provisions

***[Guidance: Please note, the reference at paragraphs 1.6.1, 1.6.2 and 1.6.4 is to Supplier Personnel to capture all individuals working on the Services. Only employees can participate in public sector pension schemes or pension schemes which are broadly comparable and therefore the information in Paragraph 1.6.3 is limited to employees]***

1. Pre-service Transfer Obligations
   1. The Supplier agrees that within 20 Working Days of the earliest of:
      1. receipt of a notification from the Authority of a Service Transfer or intended Service Transfer;
      2. receipt of the giving of notice of early termination or any Partial Termination of this Contract; and
      3. the date which is 12 months before the end of the Term; or
      4. receipt of a written request of the Authority at any time (provided that the Authority shall only be entitled to make one such request in any 6 month period),

it shall provide in a suitably anonymised format so as to comply with the DPA 2018, the Provisional Supplier Personnel List, together with the Staffing Information and it shall provide an updated Provisional Supplier Personnel List at such intervals as are reasonably requested by the Authority.

* 1. At least 20 Working Days prior to the Service Transfer Date, the Supplier shall provide to the Authority or at the direction of the Authority to any Replacement Supplier and/or any Replacement Sub-contractor:
     1. the Final Supplier Personnel List, which shall identify which of the Supplier Personnel are Transferring Supplier Employees; and
     2. the Staffing Information in relation to the Final Supplier Personnel List (insofar as such information has not previously been provided).
  2. The Authority shall be permitted to use and disclose information provided by the Supplier under Paragraphs 1.1 and 1.2 for the purpose of informing any prospective Replacement Supplier and/or Replacement Sub-contractor.
  3. The Supplier warrants, for the benefit of the Authority, any Replacement Supplier, and any Replacement Sub-contractor that all information provided pursuant to Paragraphs 1.1 and 1.2 shall be true and accurate in all material respects at the time of providing the information.
  4. From the date of the earliest event referred to in Paragraph 1.1.1, 1.1.2 and 1.1.3, the Supplier agrees, that it shall not, and agrees to procure that each Sub-contractor shall not, assign any person to the provision of the Services who is not listed on the Provisional Supplier Personnel List and shall not without the approval of the Authority (not to be unreasonably withheld or delayed):
     1. replace or re-deploy any Supplier Personnel listed on the Provisional Supplier Personnel List other than where any replacement is of equivalent grade, skills, experience and expertise and is employed on the same terms and conditions of employment as the person they replace;
     2. make, promise, propose, permit or implement any material changes to the terms and conditions of employment of the Supplier Personnel (including pensions and any payments connected with the termination of employment);
     3. increase the proportion of working time spent on the Services (or the relevant part of the Services) by any of the Supplier Personnel save for fulfilling assignments and projects previously scheduled and agreed;
     4. introduce any new contractual or customary practice concerning the making of any lump sum payment on the termination of employment of any employees listed on the Provisional Supplier Personnel List;
     5. increase or reduce the total number of employees so engaged, or deploy any other person to perform the Services (or the relevant part of the Services); or
     6. terminate or give notice to terminate the employment or contracts of any persons on the Provisional Supplier Personnel List save by due disciplinary process,

and shall promptly notify, and procure that each Sub-contractor shall promptly notify, the Authority or, at the direction of the Authority, any Replacement Supplier and any Replacement Sub-contractor of any notice to terminate employment given by the Supplier or relevant Sub-contractor or received from any persons listed on the Provisional Supplier Personnel List regardless of when such notice takes effect.

* 1. During the Term, the Supplier shall provide, and shall procure that each Sub-contractor shall provide, within 20 Working Days to the Authority any information the Authority may reasonably require relating to the manner in which the Services are organised, which shall include:
     1. the numbers of Supplier Personnel engaged in providing the Services;
     2. the percentage of time spent by each Supplier Personnel engaged in providing the Services;
     3. the extent to which each employee qualifies for membership of any of the Statutory Schemes or any Broadly Comparable scheme set up pursuant to the provisions of any of the Annexes to Part D (*Pensions*) of this Schedule 24 (*Staff Transfer*) (as appropriate); and
     4. a description of the nature of the work undertaken by each Supplier Personnel by location.
  2. The Supplier shall provide, and shall procure that each Sub-contractor shall provide, all reasonable cooperation and assistance to the Authority, any Replacement Supplier and/or any Replacement Sub-contractor to ensure the smooth transfer of the Transferring Supplier Employees on the Service Transfer Date including providing sufficient information in advance of the Service Transfer Date to ensure that all necessary payroll arrangements can be made to enable the Transferring Supplier Employees to be paid as appropriate. Without prejudice to the generality of the foregoing, within 5 Working Days following the Service Transfer Date, the Supplier shall provide, and shall procure that each Sub-contractor shall provide, to the Authority or, at the direction of the Authority, to any Replacement Supplier and/or any Replacement Sub-contractor (as appropriate), in respect of each person on the Final Supplier Personnel List who is a Transferring Supplier Employee:
     1. the most recent month’s pay slip data;
     2. details of cumulative pay for tax and pension purposes;
     3. details of cumulative tax paid;
     4. updated tax code as at the Service Transfer Date if the code has changed since it was previously provided;
     5. updated details of any voluntary deductions from pay as at the Service Transfer Date if changes have occurred since the details were previously provided;
     6. a copy of the personnel file and all other records regarding the service of the Transferring Supplier Employee;
     7. all information required to meet the minimum recording keeping requirements under the Working Time Regulations 1998 and the National Minimum Wage Regulations 2015; and
     8. updated bank/building society or other account details for payroll purposes if they have changed since they were previously provided.
  3. From the date of the earliest event referred to in Paragraph 1.1.1, 1.1.2 and 1.1.3, the Supplier agrees that following a request from the Authority it shall and shall procure that each Sub-contractor shall use reasonable endeavours to comply with any request to align and assign Supplier Personnel to any future delivery model proposed by the Authority for Replacement Services within 30 Working Days or such longer timescale as may be agreed.
  4. Any changes necessary to this Contract as a result of alignment referred to in Paragraph 1.8 shall be agreed in accordance with the Change Control Procedure.

1. Employment Regulations Exit Provisions
   1. The Authority and the Supplier acknowledge that subsequent to the commencement of the provision of the Services, the identity of the provider of the Services (or any part of the Services) may change (whether as a result of termination or Partial Termination of this Contract or otherwise) resulting in the Services being undertaken by a Replacement Supplier and/or a Replacement Sub-contractor. Such change in the identity of the supplier of such services may constitute a Relevant Transfer to which the Employment Regulations will apply. The Authority and the Supplier further agree that, as a result of the operation of the Employment Regulations, where a Relevant Transfer occurs, the contracts of employment between the Supplier and the Transferring Supplier Employees (except in relation to any contract terms disapplied through operation of regulation 10 of the Employment Regulations) will have effect on and from the Service Transfer Date as if originally made between the Replacement Supplier and/or a Replacement Sub-contractor (as the case may be) and each such Transferring Supplier Employee.
   2. The Supplier shall, and shall procure that each Sub-contractor shall, comply with all its obligations under the Employment Regulations and in particular obligations in respect of the Transferring Supplier Employees arising under the Employment Regulations in respect of the period up to (but excluding) the Service Transfer Date and shall perform and discharge, and procure that each Sub-contractor shall perform and discharge, all its obligations in respect of any person identified in the Final Supplier Personnel List arising in respect of the period up to (but excluding) the Service Transfer Date (including the payment of all remuneration, benefits, entitlements and outgoings, all wages, pay for accrued but untaken holiday, bonuses, commissions, payments of PAYE, national insurance contributions and pension contributions and all such sums due as a result of any Fair Deal Employees' participation in the Statutory Schemes and any requirement to set up a broadly comparable pension scheme which in any case are attributable in whole or in part to the period ending on (and excluding) the Service Transfer Date) and any necessary apportionments in respect of any periodic payments shall be made between:
      1. the Supplier and/or the Sub-contractor (as appropriate); and
      2. the Replacement Supplier and/or Replacement Sub-contractor.
   3. Subject to Paragraph 2.4, the Supplier shall indemnify the Authority and/or the Replacement Supplier and/or any Replacement Sub-contractor against any Employee Liabilities arising from or as a result of:
      1. any act or omission of the Supplier or any Sub-contractor in respect of any Transferring Supplier Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Supplier Employee whether occurring before, on or after the Service Transfer Date;
      2. the breach or non-observance by the Supplier or any Sub-contractor occurring before but excluding the Service Transfer Date of:
         1. any collective agreement applicable to the Transferring Supplier Employees; and/or
         2. any other custom or practice with a trade union or staff association in respect of any Transferring Supplier Employees which the Supplier or any Sub-contractor is contractually bound to honour;
      3. any claim by any trade union or other body or person representing any Transferring Supplier Employees arising from or connected with any failure by the Supplier or a Sub-contractor to comply with any legal obligation to such trade union, body or person arising before but excluding the Service Transfer Date;
      4. any proceeding, claim or demand by HMRC or other statutory authority in respect of any financial obligation including, but not limited to, PAYE and primary and secondary national insurance contributions:
         1. in relation to any Transferring Supplier Employee, to the extent that the proceeding, claim or demand by HMRC or other statutory authority relates to financial obligations arising before but excluding the Service Transfer Date; and
         2. in relation to any employee who is not identified in the Final Supplier Personnel List, and in respect of whom it is later alleged or determined that the Employment Regulations applied so as to transfer his/her employment from the Supplier to the Authority and/or Replacement Supplier and/or any Replacement Sub-contractor, to the extent that the proceeding, claim or demand by HMRC or other statutory authority relates to financial obligations arising before but excluding the Service Transfer Date;
      5. a failure of the Supplier or any Sub-contractor to discharge or procure the discharge of all wages, salaries and all other benefits and all PAYE tax deductions and national insurance contributions relating to the Transferring Supplier Employees in respect of the period up to (but excluding) the Service Transfer Date);
      6. any claim made by or in respect of any person employed or formerly employed by the Supplier or any Sub-contractor other than a Transferring Supplier Employee identified in the Final Supplier Personnel List for whom it is alleged the Authority and/or the Replacement Supplier and/or any Replacement Sub-contractor may be liable by virtue of this Contract and/or the Employment Regulations; and
      7. any claim made by or in respect of a Transferring Supplier Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Supplier Employee relating to any act or omission of the Supplier or any Sub-contractor in relation to its obligations under regulation 13 of the Employment Regulations, except to the extent that the liability arises from the failure by the Authority and/or Replacement Supplier to comply with regulation 13(4) of the Employment Regulations.
   4. The indemnities in Paragraph 2.3 shall not apply to the extent that the Employee Liabilities arise or are attributable to any act or omission of the Replacement Supplier and/or any Replacement Sub-contractor whether occurring or having its origin before, on or after the Service Transfer Date, including any Employee Liabilities:
      1. arising out of the resignation of any Transferring Supplier Employee before the Service Transfer Date on account of substantial detrimental changes to his/her terms and conditions of employment or working conditions proposed by the Replacement Supplier and/or any Replacement Sub-contractor to occur in the period on or after the Service Transfer Date); or
      2. arising from the Replacement Supplier’s failure, and/or Replacement Sub-contractor’s failure, to comply with its obligations under the Employment Regulations.
   5. If any person who is not identified in the Final Supplier Personnel List claims, or it is determined in relation to any person who is not identified in the Final Supplier Personnel List, that his/her contract of employment has been transferred from the Supplier or any Sub-contractor to the Replacement Supplier and/or Replacement Sub-contractor pursuant to the Employment Regulations, then:
      1. the Authority shall procure that the Replacement Supplier shall, or any Replacement Sub-contractor shall, within 5 Working Days of becoming aware of that fact, give notice in writing to the Supplier; and
      2. the Supplier may offer (or may procure that a Sub-contractor may offer) employment to such person within 15 Working Days of the notification by the Replacement Supplier and/or any and/or Replacement Sub-contractor or take such other reasonable steps as it considers appropriate to deal with the matter provided always that such steps are in compliance with Law.
   6. If such offer is accepted, or if the situation has otherwise been resolved by the Supplier or a Sub-contractor, the Authority shall procure that the Replacement Supplier shall, or procure that the Replacement Sub-contractor shall, immediately release or procure the release of the person from their employment or alleged employment.
   7. If after the 15 Working Day period specified in Paragraph 2.5.2 has elapsed:
      1. no such offer of employment has been made;
      2. such offer has been made but not accepted; or
      3. the situation has not otherwise been resolved

the Authority shall advise the Replacement Supplier and/or Replacement Sub-contractor, as appropriate that it may within 5 Working Days give notice to terminate the employment or alleged employment of such person.

* 1. Subject to the Replacement Supplier and/or Replacement Sub-contractor acting in accordance with the provisions of Paragraphs 2.5 to 2.7, and in accordance with all applicable proper employment procedures set out in applicable Law, the Supplier shall indemnify the Replacement Supplier and/or Replacement Sub-contractor against all Employee Liabilities arising out of the termination of employment pursuant to the provisions of Paragraph 2.7 provided that the Replacement Supplier takes, or shall procure that the Replacement Sub-contractor takes, all reasonable steps to minimise any such Employee Liabilities.
  2. The indemnity in Paragraph 2.8:
     1. shall not apply to:
        1. any claim for:
           1. any contravention of the Equality Act 2010 (or predecessor/successor legislation); or
           2. equal pay or compensation for less favourable treatment of part-time workers or fixed-term employees,

in any case in relation to any alleged act or omission of the Replacement Supplier and/or Replacement Sub-contractor; or

* + - 1. any claim that the termination of employment was unfair because the Replacement Supplier and/or Replacement Sub-contractor neglected to follow a fair dismissal procedure; and
    1. shall apply only where the notification referred to in Paragraph 2.5.1 is made by the Replacement Supplier and/or Replacement Sub-contractor to the Supplier within 6 months of the Service Transfer Date.
  1. If any such person as is described in Paragraph 2.5 is neither re-employed by the Supplier or any Sub-contractor nor dismissed by the Replacement Supplier and/or Replacement Sub-contractor within the time scales set out in Paragraphs 2.5 to 2.7, such person shall be treated as a Transferring Supplier Employee.
  2. The Supplier shall, and shall procure that each Sub-contractor shall, promptly provide to the Authority and any Replacement Supplier and/or Replacement Sub-contractor, in writing such information as is necessary to enable the Authority, the Replacement Supplier and/or Replacement Sub-contractor to carry out their respective duties under regulation 13 of the Employment Regulations. The Authority shall procure that the Replacement Supplier and/or Replacement Sub-contractor, shall promptly provide to the Supplier and each Sub-contractor in writing such information as is necessary to enable the Supplier and each Sub-contractor to carry out their respective duties under regulation 13 of the Employment Regulations.
  3. Subject to Paragraph 2.13, the Authority shall procure that the Replacement Supplier indemnifies the Supplier on its own behalf and on behalf of any Replacement Sub-contractor and its sub-contractors against any Employee Liabilities arising from or as a result of:
     1. any act or omission of the Replacement Supplier and/or Replacement Sub-contractor in respect of any Transferring Supplier Employee identified in the Final Supplier Personnel List or any appropriate employee representative (as defined in the Employment Regulations) of any such Transferring Supplier Employee;
     2. the breach or non-observance by the Replacement Supplier and/or Replacement Sub-contractor on or after the Service Transfer Date of:
        1. any collective agreement applicable to the Transferring Supplier Employees identified in the Final Supplier Personnel List; and/or
        2. any custom or practice in respect of any Transferring Supplier Employees identified in the Final Supplier Personnel List which the Replacement Supplier and/or Replacement Sub-contractor is contractually bound to honour;
     3. any claim by any trade union or other body or person representing any Transferring Supplier Employees identified in the Final Supplier Personnel List arising from or connected with any failure by the Replacement Supplier and/or Replacement Sub-contractor to comply with any legal obligation to such trade union, body or person arising on or after the Service Transfer Date;
     4. any proposal by the Replacement Supplier and/or Replacement Sub-contractor to change the terms and conditions of employment or working conditions of any Transferring Supplier Employees identified in the Final Supplier Personnel List on or after their transfer to the Replacement Supplier or Replacement Sub-contractor (as the case may be) on the Service Transfer Date, or to change the terms and conditions of employment or working conditions of any person identified in the Final Supplier Personnel List who would have been a Transferring Supplier Employee but for their resignation (or decision to treat their employment as terminated under regulation 4(9) of the Employment Regulations or otherwise) before the Service Transfer Date as a result of or for a reason connected to such proposed changes;
     5. any statement communicated to or action undertaken by the Replacement Supplier or Replacement Sub-contractor to, or in respect of, any Transferring Supplier Employee identified in the Final Supplier Personnel List on or before the Service Transfer Date regarding the Relevant Transfer which has not been agreed in advance with the Supplier in writing;
     6. any proceeding, claim or demand by HMRC or other statutory authority in respect of any financial obligation including, but not limited to, PAYE and primary and secondary national insurance contributions:
        1. in relation to any Transferring Supplier Employee identified in the Final Supplier Personnel List, to the extent that the proceeding, claim or demand by HMRC or other statutory authority relates to financial obligations arising on and after the Service Transfer Date; and
        2. in relation to any employee who is not a Transferring Supplier Employee identified in the Final Supplier Personnel List, and in respect of whom it is later alleged or determined that the Employment Regulations applied so as to transfer his/her employment from the Supplier or Sub-contractor, to the Replacement Supplier or Replacement Sub-contractor to the extent that the proceeding, claim or demand by HMRC or other statutory authority relates to financial obligations arising on and after the Service Transfer Date;
     7. a failure of the Replacement Supplier or Replacement Sub-contractor to discharge or procure the discharge of all wages, salaries and all other benefits and all PAYE tax deductions and national insurance contributions relating to the Transferring Supplier Employees identified in the Final Supplier Personnel List in respect of the period from (and including) the Service Transfer Date; and
     8. any claim made by or in respect of a Transferring Supplier Employee identified in the Final Supplier Personnel List or any appropriate employee representative (as defined in the Employment Regulations) of any such Transferring Supplier Employee relating to any act or omission of the Replacement Supplier or Replacement Sub-contractor in relation to obligations under regulation 13 of the Employment Regulations.
  4. The indemnities in Paragraph 2.12 shall not apply to the extent that the Employee Liabilities arise or are attributable to an act or omission of the Supplier and/or any Sub-contractor (as applicable) whether occurring or having its origin before, on or after the Service Transfer Date, including any Employee Liabilities arising from the failure by the Supplier and/or any Sub-contractor (as applicable) to comply with its obligations under the Employment Regulations.

## Annex E1: List of Notified Sub-contractors

## Annex E2: Staffing Information

Employee Information (Anonymised)

Name of Transferor:

Number of Employees in-scope to transfer:

1. Completion notes
   1. If you have any Key Sub-contractors, please complete all the above information for any staff employed by such Key Sub-contractor(s) in a separate spreadsheet.
   2. This spreadsheet is used to collect information from the current employer (transferor) about employees performing the relevant services to help plan for a potential TUPE transfer. Some or all of this information may be disclosed to bidders as part of a procurement process. The information should not reveal the employees’ identities.
   3. If the information cannot be included on this form, attach the additional information, such as relevant policies, and cross reference to the item number and employee number where appropriate.

|  | EMPLOYEE DETAILS & KEY TERMS | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Details | Job Title | Grade / band | Work Location | Date of Birth (dd/mm/yy) | Employment status (for example, employee, fixed-term employee, self-employed, agency worker)? | Continuous service date (dd/mm/yy) | Date employment started with existing employer |
| **Emp No 1** |  |  |  |  |  |  |  |
| **Emp No 2** |  |  |  |  |  |  |  |
| **Emp No** |  |  |  |  |  |  |  |
| **Emp No** |  |  |  |  |  |  |  |
| **Emp No** |  |  |  |  |  |  |  |
| **Emp No** |  |  |  |  |  |  |  |
| **Emp No** |  |  |  |  |  |  |  |
| **Emp No** |  |  |  |  |  |  |  |

|  | EMPLOYEE DETAILS & KEY TERMS | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Details | Contract end date (if fixed term contract or temporary contract) | Contractual notice period | Contractual weekly hours | Regular overtime hours per week | Mobility or flexibility clause in contract? | Previously TUPE transferred to organisation? If so, please specify (i) date of transfer, (ii) name of transferor, and (iii) whether ex public sector | Any collective agreements? | |
| **Emp No 1** |  |  |  |  |  |  |  | |
| **Emp No 2** |  |  |  |  |  |  |  | |
| **Emp No** |  |  |  |  |  |  |  | |
| **Emp No** |  |  |  |  |  |  |  | |
| **Emp No** |  |  |  |  |  |  |  | |
| **Emp No** |  |  |  |  |  |  |  | |
| **Emp No** |  |  |  |  |  |  |  | |

|  | ASSIGNMENT | CONTRACTUAL PAY AND BENEFITS | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Details | % of working time dedicated to the provision of services under the contract | Salary (or hourly rate of pay) | Payment interval (weekly / fortnightly / monthly) | Bonus payment for previous 12 months (please specify whether contractual or discretionary entitlement) | Pay review method | Frequency of pay reviews | Agreed pay increases | Next pay review date |
| **Emp No 1** |  |  |  |  |  |  |  |  |
| **Emp No 2** |  |  |  |  |  |  |  |  |
| **Emp No** |  |  |  |  |  |  |  |  |
| **Emp No** |  |  |  |  |  |  |  |  |
| **Emp No** |  |  |  |  |  |  |  |  |
| **Emp No** |  |  |  |  |  |  |  |  |
| **Emp No** |  |  |  |  |  |  |  |  |

|  | CONTRACTUAL PAY AND BENEFITS | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Details | Any existing or future commitment to training that has a time-off or financial implication | Car allowance (£ per year) | Lease or company car details | Any other allowances paid (e.g. shift allowance, standby allowance, travel allowance) | Private medical insurance (please specify whether single or family cover) | Life assurance (xSalary) | Long Term Disability / PHI (% of Salary | Any other benefits in kind |
| **Emp No 1** |  |  |  |  |  |  |  |  |
| **Emp No 2** |  |  |  |  |  |  |  |  |
| **Emp No** |  |  |  |  |  |  |  |  |
| **Emp No** |  |  |  |  |  |  |  |  |
| **Emp No** |  |  |  |  |  |  |  |  |
| **Emp No** |  |  |  |  |  |  |  |  |
| **Emp No** |  |  |  |  |  |  |  |  |

|  | CONTRACTUAL PAY AND BENEFITS | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Details | Annual leave entitlement (excluding bank holidays) | Bank holiday entitlement | Method of calculating holiday pay (i.e. based on fixed salary only or incl. entitlements to variable remuneration such as bonuses, allowances, commission or overtime pay?) | Maternity or paternity or shared parental leave entitlement and pay | Sick leave entitlement and pay | Redundancy pay entitlement (statutory / enhanced / contractual / discretionary) |
| **Emp No 1** |  |  |  |  |  |  |
| **Emp No 2** |  |  |  |  |  |  |
| **Emp No** |  |  |  |  |  |  |
| **Emp No** |  |  |  |  |  |  |
| **Emp No** |  |  |  |  |  |  |
| **Emp No** |  |  |  |  |  |  |
| **Emp No** |  |  |  |  |  |  |

|  | PENSIONS | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Details | Employee pension contribution rate | Employer pension contribution rate | Please provide the name of the pension scheme and a link to the pension scheme website | Is the scheme an occupational pension scheme as defined in the Pension Schemes Act 1993? | If the scheme is not an occupational pension scheme, what type of scheme is it? E.g. personal pension scheme? | Type of pension provision e.g. defined benefit (CARE or final salary, and whether a public sector scheme e.g. CSPS, NHSPS, LGPS etc. or a broadly comparable scheme) or a defined contribution scheme or an auto enrolment master trust? |
| **Emp No 1** |  |  |  |  |  |  |
| **Emp No 2** |  |  |  |  |  |  |
| **Emp No** |  |  |  |  |  |  |
| **Emp No** |  |  |  |  |  |  |
| **Emp No** |  |  |  |  |  |  |
| **Emp No** |  |  |  |  |  |  |
| **Emp No** |  |  |  |  |  |  |

|  | PENSIONS | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Details | If the Employee is in the Local Government Pension Scheme, please supply details of Fund and Administering Authority. | If the Employee is in the Civil Service Pension Scheme, please provide details of the Admission Agreement. | If the Employee is in the NHSPS, please provide details of the Direction Letter. | If the Employee is in a broadly comparable pension scheme, please supply a copy of the GAD certificate of Broad Comparability. | Did Fair Deal or any other similar pension protection for ex-public sector employees apply to the employee when they TUPE transferred into your employment? If so, what was the nature of that protection (e.g. right to participate in a public sector pension scheme, or a broadly comparable scheme, or to bulk transfer past pension service into their current scheme)? | If Fair Deal, Best Value or other pension protection applied, which public sector employer did they originally transfer out of and when? |
| **Emp No 1** |  |  |  |  |  |  |
| **Emp No 2** |  |  |  |  |  |  |
| **Emp No** |  |  |  |  |  |  |
| **Emp No** |  |  |  |  |  |  |
| **Emp No** |  |  |  |  |  |  |
| **Emp No** |  |  |  |  |  |  |
| **Emp No** |  |  |  |  |  |  |

|  | OTHER | | |
| --- | --- | --- | --- |
| Details | Security Check Level | Security Clearance Expiry date | Additional info or comments |
| **Emp No 1** |  |  |  |
| **Emp No 2** |  |  |  |
| **Emp No** |  |  |  |
| **Emp No** |  |  |  |
| **Emp No** |  |  |  |
| **Emp No** |  |  |  |
| **Emp No** |  |  |  |

Schedule 25

Deed of Guarantee

# **Schedule 25:** **Deed of** **Guarantee**

***[Guidance: This is a draft form of guarantee which can be used to procure a Guarantee, but it will need to be amended to reflect the Beneficiary’s requirements.]***

[Insert the name of the Guarantor]

- and -

[Insert the name of the Beneficiary]

DEED OF GUARANTEE

THIS DEED is executed as a deed and dated **[Insert** date of execution] (the “Deed”)

BETWEEN:

1. [INSERT NAME OF THE GUARANTOR] [a company incorporated in [England and Wales] under registered number **[insert** registered number] whose registered office is at **[insert** registered office]] [OR] [a company incorporated under the laws of **[insert** country], registered in **[insert** country] with number **[insert** number] at **[insert** place of registration], whose principal office is at **[insert** office details] (the “Guarantor”); and
2. [INSERT NAME OF THE AUTHORITY], [acting on behalf of the Crown] of **[insert** the Authority’s address] (the “Authority”).

together the “Parties” and each a “Party”.

BACKGROUND:

(A) The Authority [has awarded] a contract dated **[insert** date] to **[insert** details of the Supplier] (the “Supplier”) for the provision of **[insert** details of goods or services to be provided] (the “Guaranteed Agreement”).

(B) It is a condition of the Authority entering into the Guaranteed Agreement that the Supplier procures the execution and delivery to the Authority of a parent company guarantee substantially in the form of this Deed.

(C) The Guarantor has agreed to guarantee the due performance of the Guaranteed Agreement.

IT IS AGREED as follows:

1. Definitions and Interpretation

Definitions

* 1. The following definitions apply in this Deed:

|  |  |
| --- | --- |
| “Business Day” | means a day, other than a Saturday, Sunday or public holiday in England, when banks in London are open for business; |
| “Control” | means the power of a person to secure that the affairs of a body corporate are conducted in accordance with the wishes of that person:   1. by means of the holding of shares or the possession of voting power in relation to that body or any other body corporate; or 2. as a result of any powers conferred by the constitutional or corporate documents, or any other document regulating that body or any other body corporate; |
| “Guaranteed Agreement” | has the meaning given to it in Recital (A); |
| “Guaranteed Obligations” | has the meaning given to it in Clause 2.1.1; |
| “Supplier” | has the meaning given to it in Recital (A); |
| “VAT” | means value added tax or any equivalent tax chargeable in the UK or elsewhere. |

Interpretation

* 1. Unless otherwise stated, any reference in this Deed to:
     1. the “Guarantor”, the “Authority”, the “Supplier” or any other person shall be construed so as to include their successors in title, permitted assigns and permitted transferees, whether direct or indirect;
     2. “assets” includes present and future properties, revenues and rights of every description;
     3. this “Deed”, or any other agreement or instrument is a reference to, this deed or other agreement or instrument as amended, novated, supplemented, extended or restated;
     4. “indebtedness” includes any obligation (whether incurred as principal or as surety) for the payment or repayment of money, whether present or future, actual or contingent;
     5. a “person” includes any individual, firm, company, corporation, government, state or agency of a state or any association, trust, joint venture, consortium, partnership or other entity (whether or not having separate legal personality);
     6. the words “including”, “includes”, “in particular”, “for example” or similar shall be construed as illustrative and without limitation to the generality of the related general words; and
     7. a time of day is a reference to London time.

1. Guarantee and Indemnity
   1. The Guarantor:
      1. guarantees to the Authority the due and punctual performance of all of the Supplier’s present and future obligations under and in connection with the Guaranteed Agreement if and when they become due and performable in accordance with the terms of the Guaranteed Agreement (the “Guaranteed Obligations”);
      2. shall pay to the Authority from time to time on demand all monies (together with interest on such sum accrued before and after the date of demand until the date of payment) that have become payable by the Supplier to the Authority under or in connection with the Guaranteed Agreement but which has not been paid at the time the demand is made; and
      3. shall, if the Supplier fails to perform in full and on time any of the Guaranteed Obligations and upon written notice from the Authority, immediately on demand perform or procure performance of the same at the Guarantor’s own expense.
   2. The Guarantor, as principal obligor and as a separate and independent obligation and liability from its obligations and liabilities under Clause 2.1, shall indemnify and keep indemnified the Authority in full and on demand from and against all and any losses, damages, costs and expenses suffered or incurred by the Authority arising out of, or in connection with:
      1. any failure by the Supplier to perform or discharge the Guaranteed Obligations; or
      2. any of the Guaranteed Obligations being or becoming wholly or partially unenforceable for any reason,
      3. provided that the Guarantor’s liability under this Clause 2.2 shall be no greater than the Supplier’s liability under the Guaranteed Agreement was (or would have been had the relevant Guaranteed Obligation been fully enforceable).
2. Authority Protections

Continuing Guarantee

* 1. This Deed is, and shall at all times be, a continuing and irrevocable security until the Guaranteed Obligations have been satisfied or performed in full, and is in addition to and not in substitution for and shall not merge with any other right, remedy, guarantee or security which the Authority may at any time hold for the performance of the Guaranteed Obligations and may be enforced without first having recourse to any such security.

Preservation of the Guarantor’s liability

* 1. The Guarantor’s liability under this Deed shall not be reduced, discharged or otherwise adversely affected by:
     1. any arrangement made between the Supplier and the Authority;
     2. any partial performance (except to the extent of such partial performance) by the Supplier of the Guaranteed Obligations;
     3. any alteration in the obligations undertaken by the Supplier whether by way of any variation referred to in Clause 4 or otherwise;
     4. any waiver or forbearance by the Authority whether as to payment, time, performance or otherwise;
     5. the taking, variation, renewal or release of, the enforcement or neglect to perfect or enforce any right, guarantee, remedy or security from or against the Supplier or any other person;
     6. any unenforceability, illegality or invalidity of any of the provisions of the Guaranteed Agreement or any of the Supplier’s obligations under the Guaranteed Agreement, so that this Deed shall be construed as if there were no such unenforceability, illegality or invalidity;
     7. any dissolution, amalgamation, reconstruction, reorganisation, change in status, function, Control or ownership, insolvency, liquidation, administration, voluntary arrangement, or appointment of a receiver, of the Supplier or any other person.

Immediate demand

* 1. The Guarantor waives any right it may have to require the Authority to proceed against, enforce any other right or claim for payment against, or take any other action against, the Supplier or any other person before claiming from the Guarantor under this Guarantee.

Deferral of rights

* 1. Until all amounts which may be or become payable under the Guaranteed Agreement or this Deed have been irrevocably paid in full, the Guarantor shall not, as a result of this Deed or any payment performance under this Deed:
     1. be subrogated to any right or security of the Authority;
     2. claim or prove in competition with the Authority against the Supplier or any other person;
     3. demand or accept repayment in whole or in part of any indebtedness due from the Supplier;
     4. take the benefit of, share in or enforce any security or other guarantee or indemnity against the Supplier; or
     5. claim any right of contribution, set-off or indemnity from the Supplier,

without the prior written consent of the Authority (and in such case only in accordance with any written instructions of the Authority).

* 1. If the Guarantor receives any payment or other benefit in breach of Clause 3.4, or as a result of any action taken in accordance with a written instruction of the Authority given pursuant to Clause 3.4, such payment of other benefit, and any benefit derived directly or indirectly by the Guarantor therefrom, shall be held by the Guarantor on trust for the Authority applied towards the discharge of the Guarantor’s obligations to the Authority under this Deed.

1. Variation of the Guaranteed Agreement
   1. The Guarantor confirms that it intends that this Deed shall extend and apply from time to time to any variation, increase, extension or addition of the Guaranteed Agreement, however, fundamental, and any associated fees, costs and/or expenses.
2. Payment and Costs
   1. All sums payable by the Guarantor under this Deed shall be paid in full to the Authority in pounds sterling:
      1. without any set-off, condition or counterclaim whatsoever; and
      2. free and clear of any deductions or withholdings whatsoever except as may be required by applicable law which is binding on the Guarantor.
   2. If any deduction or withholding is required by any applicable law to be made by the Guarantor:
      1. the amount of the payment due from the Guarantor shall be increased to an amount which (after making any deduction or withholding) leaves an amount equal to the payment which would have been due if no deduction or withholding had been required; and
      2. the Guarantor shall promptly deliver to the Authority all receipts issued to it evidencing each deduction or withholding which it has made.
   3. The Guarantor shall not and may not direct the application by the Authority of any sums received by the Authority from the Guarantor under any of the terms in this Deed.
   4. The Guarantor shall pay interest on any amount due under this Deed at the applicable rate under the Late Payment of Commercial Debts (Interest) Act 1998, accruing on a daily basis from the due date up to the date of actual payment, whether before or after judgment.
   5. The Guarantor shall, on a full indemnity basis, pay to the Authority on demand the amount of all costs and expenses (including legal and out-of-pocket expenses and any VAT on those costs and expenses) which the Authority incurs in connection with:
      1. the preservation, or exercise and enforcement, of any rights under or in connection with this Deed or any attempt to do so; and
      2. any discharge or release of this Deed.
3. Conditional Discharge
   1. Any release, discharge or settlement between the Guarantor and the Authority in relation to this Deed shall be conditional on no right, security, disposition or payment to the Authority by the Guarantor, the Supplier or any other person being avoided, set aside or ordered to be refunded pursuant to any enactment or law relating to breach of duty by any person, bankruptcy, liquidation, administration, protection from creditors generally or insolvency for any other reason.
   2. If any such right, security, disposition or payment as referred to in Clause 6.1 is avoided, set aside or ordered to be refunded, the Authority shall be entitled subsequently to enforce this Deed against the Guarantor as if such release, discharge or settlement had not occurred and any such security, disposition or payment has not been made.
4. Representations and Warranties
   1. The Guarantor represents and warrants to the Authority that:
      1. it is duly incorporated with limited liability and is a validly existing company under the laws of its place of incorporation, has the capacity to sue or be sued in its own name, and has power to carry on its business as now being conducted and to own its property and other assets;
      2. it has full power under its constitution or equivalent constitutional documents in the jurisdiction in which it is established to enter into this Deed;
      3. it has full power to perform the obligations expressed to be assumed by it or contemplated by this Deed;
      4. it has been duly authorised to enter into this Deed;
      5. it has taken all necessary corporate action to authorise the execution, delivery and performance of this Deed;
      6. this Deed when executed and delivered will constitute a legally binding obligation on it enforceable in accordance with its terms;
      7. all necessary consents and authorisations for the giving and implementation of this Deed have been obtained;
      8. that its entry into and performance of its obligations under this Deed will not constitute any breach of or default under any contractual, government or public obligation binding on it; and
      9. that it is not engaged in any litigation or arbitration proceedings that might affect its capacity or ability to perform its obligations under this Deed and to the best of its knowledge no such legal or arbitration proceedings have been threatened or are pending against it.
5. Assignment
   1. The Authority shall be entitled by notice in writing to the Guarantor to assign the benefit of this Deed at any time to any person without the consent of the Guarantor being required and any such assignment shall not release the Guarantor from liability under this Deed.
   2. The Guarantor may not assign or transfer any of its rights and/or obligations under this Deed without the prior written consent of the Authority.
6. Variation
   1. No variation of this Deed shall be effective unless it is in writing and signed by the parties.
7. Demands and Notices
   1. Any demand or notice served by the Authority on the Guarantor under this Deed shall be in writing, addressed to:
      1. For the Attention of **[Insert** details]
      2. [Address of the Guarantor in England and Wales]
   2. or such other address in England and Wales as the Guarantor has from time to time notified to the Authority in writing in accordance with the terms of this Deed as being an address or facsimile number for the receipt of such demands or notices.
   3. Any notice or demand served on the Guarantor or the Authority under this Deed shall be deemed to have been served:
      1. if delivered by hand, at the time of delivery; or
      2. if posted, at 10.00 a.m. on the second Business Day after it was put into the post.
   4. In proving service of a notice or demand on the Guarantor it shall be sufficient to prove that delivery was made, or that the envelope containing the notice or demand was properly addressed and posted as a prepaid first class recorded delivery letter.
   5. Any notice purported to be served on the Authority under this Deed shall only be valid when received in writing by the Authority.
8. Entire Agreement
   1. This Deed constitutes the entire agreement between the parties and supersedes and extinguishes all previous agreements, promises, assurances, warranties, representations and understandings between them, whether written or oral, relating to its subject matter.
   2. The Guarantor acknowledges that it has not entered into this Deed in reliance upon, nor has it been induced to enter into this Deed by, any representation, warranty or undertaking made by or on behalf of the Authority (whether express or implied and whether pursuant to statute or otherwise) which is not set out in this Deed.
9. Waiver
   1. No failure or delay by the Authority to exercise any right or remedy provided under this Deed or by law shall constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of such right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.
   2. Any waiver by the Authority of any terms of this Deed, or of any Guaranteed Obligations, shall only be effective if given in writing and then only for the purpose and upon the terms and conditions, if any, on which it is given.
10. Severance
    1. If any provision or part-provision of this Deed is or becomes invalid, illegal or unenforceable for any reason, such provision or part-provision shall be deemed deleted, but that shall not affect the validity and enforceability of the rest of this Deed.
11. Third Party Rights
    1. A person who is not a Party to this Deed shall have no right under the Contracts (Rights of Third Parties) Act 1999 (as amended, updated or replaced from time to time) to enforce any of its terms but this does not affect any third party right which exists or is available independently of that Act.
12. Governing Law and Jurisdiction
    1. This Deed and any issues, disputes or claims (whether contractual or non-contractual) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the laws of England and Wales.
    2. The Guarantor irrevocably agrees for the benefit of the Authority that the courts of England shall have jurisdiction to settle any dispute or claim (whether contractual or non-contractual) that arises out of or in connection with this Deed or its subject matter or formation.
    3. Nothing contained in Clause 15.2 shall limit the rights of the Authority to take proceedings against the Guarantor in any other court of competent jurisdiction, nor shall the taking of any such proceedings in one or more jurisdictions preclude the taking of proceedings in any other jurisdiction, whether concurrently or not (unless precluded by applicable law).
    4. The Guarantor irrevocably waives any objection which it may have now or in the future to the courts of England being nominated for the purpose of this Clause on the ground of venue or otherwise and agrees not to claim that any such court is not a convenient or appropriate forum.
    5. [The Guarantor irrevocably appoints **[Insert** name of agent] of **[Insert** address of agent] as its agent to receive on its behalf in England or Wales service of any proceedings under this Clause 15. Such service shall be deemed completed on delivery to such agent (whether or not it is forwarded to and received by the Guarantor) and shall be valid until such time as the Authority has received prior written notice that such agent has ceased to act as agent. If for any reason such agent ceases to be able to act as agent or no longer has an address in England or Wales, the Guarantor shall appoint a substitute acceptable to the Authority and deliver to the Authority the new agent’s name and address within England and Wales.]

|  |  |
| --- | --- |
| Executed as a deed by **[Insert** the name of the Guarantor] acting by **[Insert** name of Director] a director, in the presence of a witness: |  |
| ……………………………………………. [Signature of Witness] | ……………………………………………. [Signature of Director]  Name of Director:  …………………………………………… |
| Name of Witness: | …………………………………………… |
| Address of Witness: | ……………………………………………  …………………………………………… |
| Occupation of Witness: | …………………………………………… |

Schedule 26

Processing Personal Data

# Schedule 26: Processing Personal Data

1. Data Processing
   1. This Schedule shall be completed by the Controller, who may take account of the view of the Processor, however the final decision as to the content of this Schedule shall be with the Authority at its absolute discretion.
   2. The contact details of the Authority’s Data Protection Officer are: [Insert Contact details]
   3. The contact details of the Supplier’s Data Protection Officer are: [Insert Contact details]
   4. The Processor shall comply with any further written instructions with respect to processing by the Controller.
   5. Any such further instructions shall be incorporated into this Schedule.

*[Guidance: The Authority will be the Controller, and the Supplier the Processor in the vast majority of cases. If the Authority believes another Personal Data Processing scenario applies, such as the Parties being Joint or Independent Controllers, the Authority must speak to its data protection team or DPO.]*

| **Description** | **Details** |
| --- | --- |
| Identity of Controller for each Category of Personal Data | The Authority is Controller and the Supplier is Processor  The Parties acknowledge that in accordance with Clauses 21.2 to 21.15 and for the purposes of the Data Protection Legislation, the Authority is the Controller and the Supplier is the Processor of the following Personal Data:  [Insert the scope of Personal Data for which the purposes and means of the Processing by the Supplier is determined by the Authority]  The Supplier is Controller and the Authority is Processor  The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Authority is the Processor in accordance with Clauses 21.2 to 21.15 of the following Personal Data:  [Insert the scope of Personal Data for which the purposes and means of the Processing by the Authority is determined by the Supplier]  The Parties are Joint Controllers  The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of:  [Insert the scope of Personal Data for which the purposes and means of the Processing is determined by both Parties together]  The Parties are Independent Controllers of Personal Data  The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:  Personally identifiable information of Supplier Personnel,  Personally identifiable information of any directors, officers, employees, agents, consultants and contractors of the Authority (excluding the Supplier Personnel) engaged in the performance of the Authority’s duties under this Contract).  [Insert the scope of other Personal Data provided by one Party who is Data Controller to the other Party who will separately determine the nature and purposes of its Processing the Personal Data on receipt.  e.g. where (1) the Supplier has professional or regulatory obligations in respect of Personal Data received, (2) a standardised service is such that the Authority cannot dictate the way in which Personal Data is Processed by the Supplier, or (3) where the Supplier comes to the transaction with Personal Data for which it is already Controller for use by the Authority] |
| Subject matter of the Processing | [This should be a high level, short description of what the Processing is about i.e. its subject matter of the contract.  Example: The processing is needed in order to ensure that the Processor can effectively deliver the contract to provide [insert description of relevant service]. |
| Duration of the Processing | [Clearly set out the duration of the processing including dates] |
| Nature and purposes of the processing | [Please be as specific as possible, but make sure that you cover all intended purposes.  The nature of the Processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.  The purpose might include: employment processing, statutory obligation, recruitment assessment etc] |
| Type of Personal Data being Processed | [Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc] |
| Categories of Data Subject | [Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc] |
| Plan for return and destruction of the data once the Processing is complete  UNLESS requirement under law to preserve that type of data | [Describe how long the data will be retained for, how it be returned or destroyed] |
| Locations at which the Supplier and/or its Sub-contractors Process Personal Data under this Contract and international transfers and legal gateway | [Clearly identify each location, explain where geographically personal data may be stored or accessed from. Explain the legal gateway you are relying on to export the data e.g. adequacy decision, EU SCCs, UK IDTA. Annex any SCCs or IDTA to this contract] |
| Protective Measures that the Supplier and, where applicable, its Sub-contractors have implemented to protect Personal Data Processed under this Contract against a breach of security (insofar as that breach of security relates to data) or a Data Loss Event (noting that any Protective Measures are to be in accordance with Schedule 5 *(Security Management)*) | [Please be as specific as possible. Any Protective Measures must be in accordance with the Security Requirements in Schedule 5 *(Security Management).*] |

## Annex 1: Joint Controller Agreement

1. Joint Controller Status and Allocation of Responsibilities
   1. With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 1 (*Joint Controller Agreement*) in replacement of Clause 21.3 to 21.15 (*Where one Party is* *Controller and the other Party is Processor*) and 21.17 to 21.28 (*Independent* *Controllers of Personal Data*). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.
   2. The Parties agree that the [Supplier/Authority]:
      1. is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;
      2. shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;
      3. is solely responsible for the Parties’ compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the UK GDPR;
      4. is responsible for obtaining the informed consent of Data Subjects, in accordance with the UK GDPR, for Processing in connection with the Services where consent is the relevant legal basis for that Processing; and
      5. shall make available to Data Subjects the essence of this Joint Controller Agreement (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the [Supplier’s/Authority’s] privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).
   3. Notwithstanding the terms of Paragraph 1.2, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Legislation as against the relevant Party as Data Controller.
2. Undertakings of Both Parties
   1. The Supplier and the Authority each undertake that they shall:
      1. report to the other Party every [x] months on:
         1. the volume of Data Subject Access Requests (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);
         2. the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;
         3. any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party’s obligations under applicable Data Protection Legislation;
         4. any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and
         5. any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law;

that it has received in relation to the subject matter of the Contract during that period;

* + 1. notify each other immediately if it receives any request, complaint or communication made as referred to in Paragraphs 2.1.1(a) to (e); and
    2. provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Paragraphs 1.2 and 2.1.1(a) to (e) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;
    3. not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under this Contract or is required by Law) that disclosure or transfer of Personal Data is otherwise considered to be lawful processing of that Personal Data in accordance with Article 6 of the UK GDPR or EU GDPR (as the context requires). For the avoidance of doubt to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;
    4. request from the Data Subject only the minimum information necessary to provide the Services and treat such extracted information as Confidential Information;
    5. ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;
    6. take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:
       1. are aware of and comply with their duties under this Annex 1 (*Joint Controller Agreement*) and those in respect of Confidential Information
       2. are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where that Party would not be permitted to do so;
       3. have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;
    7. ensure that it has in place Protective Measures as appropriate to protect against a Data Loss Event having taken account of the:
       1. nature of the data to be protected;
       2. harm that might result from a Data Loss Event;
       3. state of technological development; and
       4. cost of implementing any measures;
    8. ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that the Supplier holds;
    9. ensure that it notifies the other Party as soon as it becomes aware of a Data Loss Event; and
    10. not transfer such Personal Data outside of the UK and/or the EEA unless the prior written consent of the non-transferring Party has been obtained and the following conditions are fulfilled:
        1. the destination country (and if applicable the entity receiving the Personal Data) has been recognised as adequate by the UK government in accordance with Article 45 of the UK GDPR or DPA 2018 Section 74A and/or the transfer is in accordance with Article 45 of the EU GDPR (where applicable), provided that if the destination country of a transfer is the United States:

(A) the Supplier shall ensure that prior to the transfer of any Personal Data to the United States relying on this adequacy (including to any United States-based Sub-contractors and/or Sub-processors), the Supplier (and/or the applicable Sub-contractor and/or Sub-processor) must be self-certified and continue to be self-certified on the US Data Privacy Framework;

(B) the Supplier shall notify the Authority immediately if there are any, or there are reasonable grounds to believe there may be any, changes in respect of their and/or their Sub-contractor's or Sub-processor's position on the US Data Privacy Framework (for example if that entity ceases to be certified or is at risk of being so, or there is a strong likelihood of a competent court finding the US Data Privacy Framework unlawful), and the Supplier must then take all appropriate steps to remedy the certification and/or put in place alternative data transfer mechanisms in compliance with this Paragraph 2.1.11(a); and

(C) in the event that the Supplier (and/or the applicable Sub-contractor or Sub-processor):

(1) ceases to be certified on the US Data Privacy Framework and the Supplier does not put in place the alternative data transfer mechanisms required for compliance with this Paragraph 2.1.11(a);

(2) the US Data Privacy Framework is no longer available and the Supplier does not put in place the alternative data transfer mechanisms required for compliance with this Paragraph 2.1.11(a); and/or

(3) fails to notify the Authority of any changes to its certification status in accordance with Paragraph 2.1.11(a)(B) above,

the Authority shall have the right to terminate this Contract with immediate effect; or

* + - 1. the transferring Party has provided appropriate safeguards in relation to the transfer (whether in accordance with Article 46 of the UK GDPR or DPA 2018 Section 75 and/or Article 46 of the EU GDPR (where applicable) as agreed with the non-transferring Party which could include;
      2. where the transfer is subject to UK GDPR:
         1. the UK International Data Transfer Agreement (the “**IDTA**”) as published by the Information Commissioner’s Office [or such updated version of such IDTA as is published by the Information Commissioner’s Office under section 119A(1) of the DPA 2018 from time to time ] **OR** [and as set out in Annex 2 to Schedule 26 (*Processing Personal Data*)] ***[Guidance: See guidance notes and Annex 2 for an explanation of these options]***; or
         2. the European Commission’s Standard Contractual Clauses per decision 2021/914/EU [or such updated version of such Standard Contractual Clauses as are published by the European Commission from time to time] **OR** [set out in Annex 3 to Schedule 26 (*Processing Personal Data*) [***Guidance: See guidance notes and Annex 3*** ***for an explanation of these options]*** (the “**EU SCCs**”), together with the UK International Data Transfer Agreement Addendum to the EU SCCs (the “**Addendum**”) [or such updated version of such Addendum as is published by the Information Commissioner’s Office under section 119A(1) of the DPA 2018 from time to time] **OR** [and as set out in Annex 2 to Schedule 26 (*Processing Personal Data*)] ***[Guidance: see guidance notes and Annex 2 for an explanation of these options]***; and/or
      3. where the transfer is subject to EU GDPR, the EU SCCs,

(as well as any additional measures determined by the Controller being implemented by the importing party; and

* + - 1. the Data Subject has enforceable rights and effective legal remedies;
      2. the transferring Party complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the non-transferring Party in meeting its obligations); and
      3. the transferring Party complies with any reasonable instructions notified to it in advance by the non-transferring Party with respect to the Processing of the Personal Data; and
  1. Each Joint Controller shall use its best endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Legislation and shall not perform its obligations under this Annex in such a way as to cause the other Joint Controller to breach any of its’ obligations under applicable Data Protection Legislation to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations

1. Data Protection Breach
   1. Without prejudice to Paragraph 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Data Loss Event or circumstances that are likely to give rise to a Data Loss Event, providing the other Party and its advisors with:
      1. sufficient information and in a timescale which allows the other Party to meet any obligations to report a Data Loss Event under the Data Protection Legislation;
      2. all reasonable assistance, including:
         1. co-operation with the other Party and the Information Commissioner or any other regulatory authority investigating the Data Loss Event and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;
         2. co-operation with the other Party including taking such reasonable steps as are directed by the Authority to assist in the investigation, mitigation and remediation of a Personal Data Breach;
         3. co-ordination with the other Party regarding the management of public relations and public statements relating to the Data Loss Event;
         4. providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner or any other regulatory authority investigating the Data Loss Event, with complete information relating to the Data Loss Event, including, without limitation, the information set out in Paragraph 3.2.
   2. Each Party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Data Loss Event which is the fault of that Party, as if it was that Party’s own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Data Loss Event, including providing the other Party, as soon as possible and within 48 hours of the Data Loss Event relating to the Data Loss Event, in particular:
      1. the nature of the Data Loss Event;
      2. the nature of Personal Data affected;
      3. the categories and number of Data Subjects concerned;
      4. the name and contact details of the Supplier’s Data Protection Officer or other relevant contact from whom more information may be obtained;
      5. measures taken or proposed to be taken to address the Data Loss Event; and
      6. describe the likely consequences of the Data Loss Event.
2. Audit
   1. The Supplier shall permit:
      1. the Authority, or a third-party auditor acting under the Authority’s direction, to conduct, at the Authority’s cost, data privacy and security audits, assessments and inspections concerning the Supplier’s data security and privacy procedures relating to Personal Data, its compliance with this Annex 1 and the Data Protection Legislation.
      2. the Authority, or a third-party auditor acting under the Authority’s direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 of the UK GDPR by the Supplier so far as relevant to the Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Services.
   2. The Authority may, in its sole discretion, require the Supplier to provide evidence of the Supplier’s compliance with Paragraph 4.1 in lieu of conducting such an audit, assessment or inspection.
3. Impact Assessments
   1. The Parties shall:
      1. provide all reasonable assistance to each other to prepare any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and
      2. maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with this Contract, in accordance with the terms of Article 30 of the UK GDPR.
4. ICO Guidance

The Parties agree to take account of any guidance issued by the Information Commissioner or any other regulatory authority. The Authority may on not less than thirty (30) Working Days’ notice to the Supplier amend this Contract to ensure that it complies with any guidance issued by the Information Commissioner or any other regulatory authority.

1. Liabilities for Data Protection Breach

*[Guidance:* ***This paragraph represents a risk share, you may wish to reconsider the apportionment of liability and whether recoverability of losses are likely to be hindered by the contractual limitation of liability provisions.]***

* 1. If financial penalties are imposed by the Information Commissioner or any other regulatory authority on either the Authority or the Supplier for a Data Loss Event (“Financial Penalties”) then the following shall occur:
     1. If in the view of the Information Commissioner or any other regulatory authority, the Authority is responsible for the Data Loss Event, in that it is caused as a result of the actions or inaction of the Authority, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Authority, then the Authority shall be responsible for the payment of such Financial Penalties. In this case, the Authority will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such data incident. The Supplier shall provide to the Authority and its third party investigators and auditors, on request and at the Supplier’s reasonable cost, full cooperation and access to conduct a thorough audit of such data incident;
     2. If in the view of the Information Commissioner or any other regulatory authority, the Supplier is responsible for the Data Loss Event, in that it is not a breach that the Authority is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Authority and its auditors, on request and at the Supplier’s sole cost, full cooperation and access to conduct a thorough audit of such data incident; or
     3. If no view as to responsibility is expressed by the Information Commissioner or any other regulatory authority, then the Authority and the Supplier shall work together to investigate the relevant data incident and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any Financial Penalties equally if no responsibility for the Data Loss Event can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Schedule 19 (*Dispute Resolution Procedure*).
  2. If either the Authority or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction (“Court”) by a third party in respect of a Data Loss Event, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Data Loss Event shall be liable for the losses arising from such breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.
  3. In respect of any losses, cost claims or expenses incurred by either Party as a result of a Data Loss Event (the “Claim Losses”):
     1. if the Authority is responsible for the relevant breach, then the Authority shall be responsible for the Claim Losses;
     2. if the Supplier is responsible for the relevant breach, then the Supplier shall be responsible for the Claim Losses; and
     3. if responsibility is unclear, then the Authority and the Supplier shall be responsible for the Claim Losses equally.
  4. Nothing in Paragraphs 7.2 to 7.3 shall preclude the Authority and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Data Loss Event, having regard to all the circumstances of the breach and the legal and financial obligations of the Authority.

1. Termination
   1. If the Supplier is in material Default under any of its obligations under this Annex 1 (*Joint Controller Agreement*), the Authority shall be entitled to terminate this Contract by issuing a Termination Notice to the Supplier in accordance with Clause 31 (*Termination Rights*).
2. Sub-Processing
   1. In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:
      1. carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by this Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and
      2. ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.
3. Data Retention
   1. The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Legislation and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by a Party for statutory compliance purposes or as otherwise required by this Contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy.

## Annex 2: International Data Transfer Agreement and International Data Transfer Agreement Addendum to the EU Commission Standard Contractual Clauses

## Part A: International Data Transfer Agreement

***[Guidance: Delete this Annex and replace with the text ‘NOT USED’ if the Authority has chosen to refer out to the IDTA, rather than incorporating the text, that is, by selecting the first set of square brackets in Clause 21 of the Core Terms and in this Schedule.]***



Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

International Data Transfer Agreement

**VERSION A1.0, in force 21 March 2022**

This IDTA has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

### Part 1: Tables

**Table 1: Parties and signatures**

|  |  |
| --- | --- |
| **Start date** |  |

| The Parties | Exporter (who sends the Restricted Transfer) | Importer (who receives the Restricted Transfer) |
| --- | --- | --- |
| **Parties’ details** | Full legal name:  Trading name (if different):  Main address (if a company registered address):  Official registration number (if any) (company number or similar identifier): | Full legal name:  Trading name (if different):  Main address (if a company registered address):  Official registration number (if any) (company number or similar identifier): |
| **Key Contact** | Full Name (optional):  Job Title:  Contact details including email: | Full Name (optional):  Job Title:  Contact details including email: |
| **Importer Data Subject Contact** |  | Job Title:  Contact details including email: |
| **Signatures confirming each Party agrees to be bound by this IDTA** | Signed for and on behalf of the **Exporter** set out above  Signed:  Date of signature:  Full name:  Job title: | Signed for and on behalf of the **Importer** set out above  Signed:  Date of signature:  Full name:  Job title: |

**Table 2: Transfer Details**

|  |  |
| --- | --- |
| **UK country’s law that governs the IDTA:** | England and Wales  Northern Ireland  Scotland |
| **Primary place for legal claims to be made by the Parties** | England and Wales  Northern Ireland  Scotland |
| **The status of the Exporter** | In relation to the Processing of the Transferred Data:  Exporter is a Controller  Exporter is a Processor or Sub-Processor |
| **The status of the Importer** | In relation to the Processing of the Transferred Data:  Importer is a Controller  Importer is the Exporter’s Processor or Sub-Processor  Importer is **not** the Exporter’s Processor or Sub-Processor (and the Importer has been instructed by a Third Party Controller) |
| **Whether UK GDPR applies to the Importer** | UK GDPR applies to the Importer’s Processing of the Transferred Data  UK GDPR does not apply to the Importer’s Processing of the Transferred Data |
| **Linked Agreement** | **If the Importer is the Exporter’s Processor or Sub-Processor** – the agreement(s) between the Parties which sets out the Processor’s or Sub-Processor’s instructions for Processing the Transferred Data:  Name of agreement:  Date of agreement:  Parties to the agreement:  Reference (if any):  **Other agreements** – any agreement(s) between the Parties which set out additional obligations in relation to the Transferred Data, such as a data sharing agreement or service agreement:  Name of agreement:  Date of agreement:  Parties to the agreement:  Reference (if any):  **If the Exporter is a Processor or Sub-Processor** – the agreement(s) between the Exporter and the Party(s) which sets out the Exporter’s instructions for Processing the Transferred Data:  Name of agreement:  Date of agreement:  Parties to the agreement:  Reference (if any): |
| **Term** | The Importer may Process the Transferred Data for the following time period:  the period for which the Linked Agreement is in force  time period:  (only if the Importer is a Controller or not the Exporter’s Processor or Sub-Processor) no longer than is necessary for the Purpose. |
| **Ending the IDTA before the end of the Term** | the Parties cannot end the IDTA before the end of the Term unless there is a breach of the IDTA or the Parties agree in writing.  the Parties can end the IDTA before the end of the Term by serving:        months’ written notice, as set out in Section 29 (How to end this IDTA without there being a breach). |
| **Ending the IDTA when the Approved IDTA changes** | Which Parties may end the IDTA as set out in Section 29.2:  Importer  Exporter  neither Party |
| **Can the Importer make further transfers of the Transferred Data?** | The Importer MAY transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data).  The Importer MAY NOT transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data). |
| **Specific restrictions when the Importer may transfer on the Transferred Data** | The Importer MAY ONLY forward the Transferred Data in accordance with Section 16.1:  if the Exporter tells it in writing that it may do so.  to:  to the authorised receivers (or the categories of authorised receivers) set out in:  there are no specific restrictions. |
| **Review Dates** | No review is needed as this is a one-off transfer and the Importer does not retain any Transferred Data  First review date:  The Parties must review the Security Requirements at least once:  each       month(s)  each quarter  each 6 months  each year  each       year(s)  each time there is a change to the Transferred Data, Purposes, Importer Information, TRA or risk assessment |

**Table 3: Transferred Data**

|  |  |
| --- | --- |
| **Transferred Data** | The personal data to be sent to the Importer under this IDTA consists of:  The categories of Transferred Data will update automatically if the information is updated in the Linked Agreement referred to.  The categories of Transferred Data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3. |
| **Special Categories of Personal Data and criminal convictions and offences** | The Transferred Data includes data relating to:  racial or ethnic origin  political opinions  religious or philosophical beliefs  trade union membership  genetic data  biometric data for the purpose of uniquely identifying a natural person  physical or mental health  sex life or sexual orientation  criminal convictions and offences  none of the above  set out in:  And:  The categories of special category and criminal records data will update automatically if the information is updated in the Linked Agreement referred to.  The categories of special category and criminal records data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3. |
| **Relevant Data Subjects** | The Data Subjects of the Transferred Data are:  The categories of Data Subjects will update automatically if the information is updated in the Linked Agreement referred to.  The categories of Data Subjects will not update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3. |
| **Purpose** | The Importer may Process the Transferred Data for the following purposes:  The Importer may Process the Transferred Data for the purposes set out in:  In both cases, any other purposes which are compatible with the purposes set out above.  The purposes will update automatically if the information is updated in the Linked Agreement referred to.  The purposes will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3. |

**Table 4: Security Requirements**

|  |  |
| --- | --- |
| **Security of Transmission** |  |
| **Security of Storage** |  |
| **Security of Processing** |  |
| **Organisational security measures** |  |
| **Technical security minimum requirements** |  |
| **Updates to the Security Requirements** | The Security Requirements will update automatically if the information is updated in the Linked Agreement referred to.  The Security Requirements will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3. |

### Part 2: Extra Protection Clauses

|  |  |
| --- | --- |
| **Extra Protection Clauses:** |  |
| **(i) Extra technical security protections** |  |
| **(ii) Extra organisational protections** |  |
| **(iii) Extra contractual protections** |  |

### Part 3: Commercial Clauses

|  |  |
| --- | --- |
| **Commercial Clauses** |  |

### Part 4: Mandatory Clauses

**Information that helps you to understand this IDTA**

1. This IDTA and Linked Agreements
   1. Each Party agrees to be bound by the terms and conditions set out in the IDTA, in exchange for the other Party also agreeing to be bound by the IDTA.
   2. This IDTA is made up of:
      1. Part one: Tables;
      2. Part two: Extra Protection Clauses;
      3. Part three: Commercial Clauses; and
      4. Part four: Mandatory Clauses.
   3. The IDTA starts on the Start Date and ends as set out in Sections 29 or 30.
   4. If the Importer is a Processor or Sub-Processor instructed by the Exporter: the Exporter must ensure that, on or before the Start Date and during the Term, there is a Linked Agreement which is enforceable between the Parties and which complies with Article 28 UK GDPR (and which they will ensure continues to comply with Article 28 UK GDPR).
   5. References to the Linked Agreement or to the Commercial Clauses are to that Linked Agreement or to those Commercial Clauses only in so far as they are consistent with the Mandatory Clauses.
2. Legal meaning of words
   1. If a word starts with a capital letter it has the specific meaning set out in the Legal Glossary in Section 36.
   2. To make it easier to read and understand, this IDTA contains headings and guidance notes. Those are not part of the binding contract which forms the IDTA.
3. You have provided all the information required
   1. The Parties must ensure that the information contained in Part one: Tables is correct and complete at the Start Date and during the Term.
   2. In Table 2: Transfer Details, if the selection that the Parties are Controllers, Processors or Sub-Processors is wrong (either as a matter of fact or as a result of applying the UK Data Protection Laws) then:
      1. the terms and conditions of the Approved IDTA which apply to the correct option which was not selected will apply; and
      2. the Parties and any Relevant Data Subjects are entitled to enforce the terms and conditions of the Approved IDTA which apply to that correct option.
   3. In Table 2: Transfer Details, if the selection that the UK GDPR applies is wrong (either as a matter of fact or as a result of applying the UK Data Protection Laws), then the terms and conditions of the IDTA will still apply to the greatest extent possible.
4. How to sign the IDTA
   1. The Parties may choose to each sign (or execute):
      1. the same copy of this IDTA;
      2. two copies of the IDTA. In that case, each identical copy is still an original of this IDTA, and together all those copies form one agreement;
      3. a separate, identical copy of the IDTA. In that case, each identical copy is still an original of this IDTA, and together all those copies form one agreement,

unless signing (or executing) in this way would mean that the IDTA would not be binding on the Parties under Local Laws.

1. Changing this IDTA
   1. Each Party must not change the Mandatory Clauses as set out in the Approved IDTA, except only:
      1. to ensure correct cross-referencing: cross-references to Part one: Tables (or any Table), Part two: Extra Protections, and/or Part three: Commercial Clauses can be changed where the Parties have set out the information in a different format, so that the cross-reference is to the correct location of the same information, or where clauses have been removed as they do not apply, as set out below;
      2. to remove those Sections which are expressly stated not to apply to the selections made by the Parties in Table 2: Transfer Details, that the Parties are Controllers, Processors or Sub-Processors and/or that the Importer is subject to, or not subject to, the UK GDPR. The Exporter and Importer understand and acknowledge that any removed Sections may still apply and form a part of this IDTA if they have been removed incorrectly, including because the wrong selection is made in Table 2: Transfer Details;
      3. so the IDTA operates as a multi-party agreement if there are more than two Parties to the IDTA. This may include nominating a lead Party or lead Parties which can make decisions on behalf of some or all of the other Parties which relate to this IDTA (including reviewing Table 4: Security Requirements and Part two: Extra Protection Clauses, and making updates to Part one: Tables (or any Table), Part two: Extra Protection Clauses, and/or Part three: Commercial Clauses); and/or
      4. to update the IDTA to set out in writing any changes made to the Approved IDTA under Section 5.4, if the Parties want to. The changes will apply automatically without updating them as described in Section 5.4;

provided that the changes do not reduce the Appropriate Safeguards.

* 1. If the Parties wish to change the format of the information included in Part one: Tables, Part two: Extra Protection Clauses or Part three: Commercial Clauses of the Approved IDTA, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
  2. If the Parties wish to change the information included in Part one: Tables, Part two: Extra Protection Clauses or Part three: Commercial Clauses of this IDTA (or the equivalent information), they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
  3. From time to time, the ICO may publish a revised Approved IDTA which:
     1. makes reasonable and proportionate changes to the Approved IDTA, including correcting errors in the Approved IDTA; and/or
     2. reflects changes to UK Data Protection Laws.

The revised Approved IDTA will specify the start date from which the changes to the Approved IDTA are effective and whether an additional Review Date is required as a result of the changes. This IDTA is automatically amended as set out in the revised Approved IDTA from the start date specified.

1. Understanding this IDTA
   1. This IDTA must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties’ obligation to provide the Appropriate Safeguards.
   2. If there is any inconsistency or conflict between UK Data Protection Laws and this IDTA, the UK Data Protection Laws apply.
   3. If the meaning of the IDTA is unclear or there is more than one meaning, the meaning which most closely aligns with the UK Data Protection Laws applies.
   4. Nothing in the IDTA (including the Commercial Clauses or the Linked Agreement) limits or excludes either Party’s liability to Relevant Data Subjects or to the ICO under this IDTA or under UK Data Protection Laws.
   5. If any wording in Parts one, two or three contradicts the Mandatory Clauses, and/or seeks to limit or exclude any liability to Relevant Data Subjects or to the ICO, then that wording will not apply.
   6. The Parties may include provisions in the Linked Agreement which provide the Parties with enhanced rights otherwise covered by this IDTA. These enhanced rights may be subject to commercial terms, including payment, under the Linked Agreement, but this will not affect the rights granted under this IDTA.
   7. If there is any inconsistency or conflict between this IDTA and a Linked Agreement or any other agreement, this IDTA overrides that Linked Agreement or any other agreements, even if those agreements have been negotiated by the Parties. The exceptions to this are where (and in so far as):
      1. the inconsistent or conflicting terms of the Linked Agreement or other agreement provide greater protection for the Relevant Data Subject’s rights, in which case those terms will override the IDTA; and
      2. a Party acts as Processor and the inconsistent or conflicting terms of the Linked Agreement are obligations on that Party expressly required by Article 28 UK GDPR, in which case those terms will override the inconsistent or conflicting terms of the IDTA in relation to Processing by that Party as Processor.
   8. The words “include”, “includes”, “including”, “in particular” are used to set out examples and not to set out a finite list.
   9. References to:
      1. singular or plural words or people, also includes the plural or singular of those words or people;
      2. legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this IDTA has been signed; and
      3. any obligation not to do something, includes an obligation not to allow or cause that thing to be done by anyone else.
2. Which laws apply to this IDTA
   1. This IDTA is governed by the laws of the UK country set out in Table 2: Transfer Details. If no selection has been made, it is the laws of England and Wales. This does not apply to Section 35 which is always governed by the laws of England and Wales.

**How this IDTA provides Appropriate Safeguards**

1. The Appropriate Safeguards
   1. The purpose of this IDTA is to ensure that the Transferred Data has Appropriate Safeguards when Processed by the Importer during the Term. This standard is met when and for so long as:
      1. both Parties comply with the IDTA, including the Security Requirements and any Extra Protection Clauses; and
      2. the Security Requirements and any Extra Protection Clauses provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach, including considering any Special Category Data within the Transferred Data.
   2. The Exporter must:
      1. ensure and demonstrate that this IDTA (including any Security Requirements and Extra Protection Clauses) provides Appropriate Safeguards; and
      2. (if the Importer reasonably requests) provide it with a copy of any TRA.
   3. The Importer must:
      1. before receiving any Transferred Data, provide the Exporter with all relevant information regarding Local Laws and practices and the protections and risks which apply to the Transferred Data when it is Processed by the Importer, including any information which may reasonably be required for the Exporter to carry out any TRA (the “Importer Information”);
      2. co-operate with the Exporter to ensure compliance with the Exporter’s obligations under the UK Data Protection Laws;
      3. review whether any Importer Information has changed, and whether any Local Laws contradict its obligations in this IDTA and take reasonable steps to verify this, on a regular basis. These reviews must be at least as frequent as the Review Dates; and
      4. inform the Exporter as soon as it becomes aware of any Importer Information changing, and/or any Local Laws which may prevent or limit the Importer complying with its obligations in this IDTA. This information then forms part of the Importer Information.
   4. The Importer must ensure that at the Start Date and during the Term:
      1. the Importer Information is accurate;
      2. it has taken reasonable steps to verify whether there are any Local Laws which contradict its obligations in this IDTA or any additional information regarding Local Laws which may be relevant to this IDTA.
   5. Each Party must ensure that the Security Requirements and Extra Protection Clauses provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.
2. Reviews to ensure the Appropriate Safeguards continue
   1. Each Party must:
      1. review this IDTA (including the Security Requirements and Extra Protection Clauses and the Importer Information) at regular intervals, to ensure that the IDTA remains accurate and up to date and continues to provide the Appropriate Safeguards. Each Party will carry out these reviews as frequently as the relevant Review Dates or sooner; and
      2. inform the other party in writing as soon as it becomes aware if any information contained in either this IDTA, any TRA or Importer Information is no longer accurate and up to date.
   2. If, at any time, the IDTA no longer provides Appropriate Safeguards the Parties must Without Undue Delay:
      1. pause transfers and Processing of Transferred Data whilst a change to the Tables is agreed. The Importer may retain a copy of the Transferred Data during this pause, in which case the Importer must carry out any Processing required to maintain, so far as possible, the measures it was taking to achieve the Appropriate Safeguards prior to the time the IDTA no longer provided Appropriate Safeguards, but no other Processing;
      2. agree a change to Part one: Tables or Part two: Extra Protection Clauses which will maintain the Appropriate Safeguards (in accordance with Section 5); and
      3. where a change to Part one: Tables or Part two: Extra Protection Clauses which maintains the Appropriate Safeguards cannot be agreed, the Exporter must end this IDTA by written notice on the Importer.
3. The ICO
   1. Each Party agrees to comply with any reasonable requests made by the ICO in relation to this IDTA or its Processing of the Transferred Data.
   2. The Exporter will provide a copy of any TRA, the Importer Information and this IDTA to the ICO, if the ICO requests.
   3. The Importer will provide a copy of any Importer Information and this IDTA to the ICO, if the ICO requests.

**The Exporter**

1. Exporter’s obligations
   1. The Exporter agrees that UK Data Protection Laws apply to its Processing of the Transferred Data, including transferring it to the Importer.
   2. The Exporter must:
      1. comply with the UK Data Protection Laws in transferring the Transferred Data to the Importer;
      2. comply with the Linked Agreement as it relates to its transferring the Transferred Data to the Importer; and
      3. carry out reasonable checks on the Importer’s ability to comply with this IDTA, and take appropriate action including under Section 9.2, Section 29 or Section 30, if at any time it no longer considers that the Importer is able to comply with this IDTA or to provide Appropriate Safeguards.
   3. The Exporter must comply with all its obligations in the IDTA, including any in the Security Requirements, and any Extra Protection Clauses and any Commercial Clauses.
   4. The Exporter must co-operate with reasonable requests of the Importer to pass on notices or other information to and from Relevant Data Subjects or any Third Party Controller where it is not reasonably practical for the Importer to do so. The Exporter may pass these on via a third party if it is reasonable to do so.
   5. The Exporter must co-operate with and provide reasonable assistance to the Importer, so that the Importer is able to comply with its obligations to the Relevant Data Subjects under Local Law and this IDTA.

**The Importer**

1. General Importer obligations
   1. The Importer must:
      1. only Process the Transferred Data for the Purpose;
      2. comply with all its obligations in the IDTA, including in the Security Requirements, any Extra Protection Clauses and any Commercial Clauses;
      3. comply with all its obligations in the Linked Agreement which relate to its Processing of the Transferred Data;
      4. keep a written record of its Processing of the Transferred Data, which demonstrate its compliance with this IDTA, and provide this written record if asked to do so by the Exporter;
      5. if the Linked Agreement includes rights for the Exporter to obtain information or carry out an audit, provide the Exporter with the same rights in relation to this IDTA; and
      6. if the ICO requests, provide the ICO with the information it would be required on request to provide to the Exporter under this Section 12.1 (including the written record of its Processing, and the results of audits and inspections).
   2. The Importer must co-operate with and provide reasonable assistance to the Exporter and any Third Party Controller, so that the Exporter and any Third Party Controller are able to comply with their obligations under UK Data Protection Laws and this IDTA.
2. Importer’s obligations if it is subject to the UK Data Protection Laws
   1. If the Importer’s Processing of the Transferred Data is subject to UK Data Protection Laws, it agrees that:
      1. UK Data Protection Laws apply to its Processing of the Transferred Data, and the ICO has jurisdiction over it in that respect; and
      2. it has and will comply with the UK Data Protection Laws in relation to the Processing of the Transferred Data.
   2. If Section 13.1 applies and the Importer complies with Section 13.1, it does not need to comply with:
      1. Section 14 (Importer’s obligations to comply with key data protection principles);
      2. Section 15 (What happens if there is an Importer Personal Data Breach);
      3. Section 15 (How Relevant Data Subjects can exercise their data subject rights); and
      4. Section 21 (How Relevant Data Subjects can exercise their data subject rights – if the Importer is the Exporter’s Processor or Sub-Processor).
3. Importer’s obligations to comply with key data protection principles
   1. The Importer does not need to comply with this Section 14 if it is the Exporter’s Processor or Sub-Processor.
   2. The Importer must:
      1. ensure that the transferred data it Processes is adequate, relevant and limited to what is necessary for the Purpose;
      2. ensure that the transferred data it Processes is accurate and (where necessary) kept up to date, and (where appropriate considering the Purposes) correct or delete any inaccurate Transferred Data it becomes aware of Without Undue Delay; and
      3. ensure that it Processes the Transferred Data for no longer than is reasonably necessary for the Purpose.
4. What happens if there is an Importer Personal Data Breach
   1. If there is an Importer Personal Data Breach, the Importer must:
      1. take reasonable steps to fix it, including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again. If the Importer is the Exporter’s Processor or Sub-Processor: these steps must comply with the Exporter’s instructions and the Linked Agreement and be in co-operation with the Exporter and any Third Party Controller; and
      2. ensure that the Security Requirements continue to provide (or are changed in accordance with this IDTA so they do provide) a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.
   2. If the Importer is a Processor or Sub-Processor: if there is an Importer Personal Data Breach, the Importer must:
      1. notify the Exporter Without Undue Delay after becoming aware of the breach, providing the following information:
         1. a description of the nature of the Importer Personal Data Breach;
         2. (if and when possible) the categories and approximate number of Data Subjects and Transferred Data records concerned;
         3. likely consequences of the Importer Personal Data Breach;
         4. steps taken (or proposed to be taken) to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Appropriate Safeguards are in place;
         5. contact point for more information; and
         6. any other information reasonably requested by the Exporter,
      2. if it is not possible for the Importer to provide all the above information at the same time, it may do so in phases, Without Undue Delay; and
      3. assist the Exporter (and any Third Party Controller) so the Exporter (or any Third Party Controller) can inform Relevant Data Subjects or the ICO or any other relevant regulator or authority about the Importer Personal Data Breach Without Undue Delay.
   3. If the Importer is a Controller: if the Importer Personal Data Breach is likely to result in a risk to the rights or freedoms of any Relevant Data Subject the Importer must notify the Exporter Without Undue Delay after becoming aware of the breach, providing the following information:
      1. a description of the nature of the Importer Personal Data Breach;
      2. (if and when possible) the categories and approximate number of Data Subjects and Transferred Data records concerned;
      3. likely consequences of the Importer Personal Data Breach;
      4. steps taken (or proposed to be taken) to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Appropriate Safeguards are in place;
      5. contact point for more information; and
      6. any other information reasonably requested by the Exporter.

If it is not possible for the Importer to provide all the above information at the same time, it may do so in phases, Without Undue Delay.

* 1. If the Importer is a Controller: if the Importer Personal Data Breach is likely to result in a high risk to the rights or freedoms of any Relevant Data Subject, the Importer must inform those Relevant Data Subjects Without Undue Delay, except in so far as it requires disproportionate effort, and provided the Importer ensures that there is a public communication or similar measures whereby Relevant Data Subjects are informed in an equally effective manner.
  2. The Importer must keep a written record of all relevant facts relating to the Importer Personal Data Breach, which it will provide to the Exporter and the ICO on request.

This record must include the steps it takes to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Security Requirements continue to provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

1. Transferring on the Transferred Data
   1. The Importer may only transfer on the Transferred Data to a third party if it is permitted to do so in Table 2: Transfer Details Table, the transfer is for the Purpose, the transfer does not breach the Linked Agreement, and one or more of the following apply:
      1. the third party has entered into a written contract with the Importer containing the same level of protection for Data Subjects as contained in this IDTA (based on the role of the recipient as controller or processor), and the Importer has conducted a risk assessment to ensure that the Appropriate Safeguards will be protected by that contract; or
      2. the third party has been added to this IDTA as a Party; or
      3. if the Importer was in the UK, transferring on the Transferred Data would comply with Article 46 UK GDPR; or
      4. if the Importer was in the UK transferring on the Transferred Data would comply with one of the exceptions in Article 49 UK GDPR; or
      5. the transfer is to the UK or an Adequate Country.
   2. The Importer does not need to comply with Section 16.1 if it is transferring on Transferred Data and/or allowing access to the Transferred Data in accordance with Section 23 (Access Requests and Direct Access).
2. Importer’s responsibility if it authorises others to perform its obligations
   1. The Importer may sub-contract its obligations in this IDTA to a Processor or Sub-Processor (provided it complies with Section 16).
   2. If the Importer is the Exporter’s Processor or Sub-Processor: it must also comply with the Linked Agreement or be with the written consent of the Exporter.
   3. The Importer must ensure that any person or third party acting under its authority, including a Processor or Sub-Processor, must only Process the Transferred Data on its instructions.
   4. The Importer remains fully liable to the Exporter, the ICO and Relevant Data Subjects for its obligations under this IDTA where it has sub-contracted any obligations to its Processors and Sub-Processors, or authorised an employee or other person to perform them (and references to the Importer in this context will include references to its Processors, Sub-Processors or authorised persons).

**What rights do individuals have?**

1. The right to a copy of the IDTA
   1. If a Party receives a request from a Relevant Data Subject for a copy of this IDTA:
      1. it will provide the IDTA to the Relevant Data Subject and inform the other Party, as soon as reasonably possible;
      2. it does not need to provide copies of the Linked Agreement, but it must provide all the information from those Linked Agreements referenced in the Tables;
      3. it may redact information in the Tables or the information provided from the Linked Agreement if it is reasonably necessary to protect business secrets or confidential information, so long as it provides the Relevant Data Subject with a summary of those redactions so that the Relevant Data Subject can understand the content of the Tables or the information provided from the Linked Agreement.
2. The right to Information about the Importer and its Processing
   1. The Importer does not need to comply with this Section 19 if it is the Exporter’s Processor or Sub-Processor.
   2. The Importer must ensure that each Relevant Data Subject is provided with details of:
      1. the Importer (including contact details and the Importer Data Subject Contact);
      2. the Purposes; and
      3. any recipients (or categories of recipients) of the Transferred Data;

The Importer can demonstrate it has complied with this Section 19.2 if the information is given (or has already been given) to the Relevant Data Subjects by the Exporter or another party.

The Importer does not need to comply with this Section 19.2 in so far as to do so would be impossible or involve a disproportionate effort, in which case, the Importer must make the information publicly available.

* 1. The Importer must keep the details of the Importer Data Subject Contact up to date and publicly available. This includes notifying the Exporter in writing of any such changes.
  2. The Importer must make sure those contact details are always easy to access for all Relevant Data Subjects and be able to easily communicate with Data Subjects in the English language Without Undue Delay.

1. How Relevant Data Subjects can exercise their data subject rights
   1. The Importer does not need to comply with this Section 20 if it is the Exporter’s Processor or Sub-Processor.
   2. If an individual requests, the Importer must confirm whether it is Processing their Personal Data as part of the Transferred Data.
   3. The following Sections of this Section 20, relate to a Relevant Data Subject’s Personal Data which forms part of the Transferred Data the Importer is Processing.
   4. If the Relevant Data Subject requests, the Importer must provide them with a copy of their Transferred Data:
      1. Without Undue Delay (and in any event within one month);
      2. at no greater cost to the Relevant Data Subject than it would be able to charge if it were subject to the UK Data Protection Laws;
      3. in clear and plain English that is easy to understand; and
      4. in an easily accessible form
      5. together with
      6. (if needed) a clear and plain English explanation of the Transferred Data so that it is understandable to the Relevant Data Subject; and
      7. information that the Relevant Data Subject has the right to bring a claim for compensation under this IDTA.
   5. If a Relevant Data Subject requests, the Importer must:
      1. rectify inaccurate or incomplete Transferred Data;
      2. erase Transferred Data if it is being Processed in breach of this IDTA;
      3. cease using it for direct marketing purposes; and
      4. comply with any other reasonable request of the Relevant Data Subject, which the Importer would be required to comply with if it were subject to the UK Data Protection Laws.
   6. The Importer must not use the Transferred Data to make decisions about the Relevant Data Subject based solely on automated Processing, including profiling (the “Decision-Making”), which produce legal effects concerning the Relevant Data Subject or similarly significantly affects them, except if it is permitted by Local Law and:
      1. the Relevant Data Subject has given their explicit consent to such Decision-Making; or
      2. Local Law has safeguards which provide sufficiently similar protection for the Relevant Data Subjects in relation to such Decision-Making, as to the relevant protection the Relevant Data Subject would have if such Decision-Making was in the UK; or
      3. the Extra Protection Clauses provide safeguards for the Decision-Making which provide sufficiently similar protection for the Relevant Data Subjects in relation to such Decision-Making, as to the relevant protection the Relevant Data Subject would have if such Decision-Making was in the UK.
2. How Relevant Data Subjects can exercise their data subject rights– if the Importer is the Exporter’s Processor or Sub-Processor
   1. Where the Importer is the Exporter’s Processor or Sub-Processor: If the Importer receives a request directly from an individual which relates to the Transferred Data it must pass that request on to the Exporter Without Undue Delay. The Importer must only respond to that individual as authorised by the Exporter or any Third Party Controller.
3. Rights of Relevant Data Subjects are subject to the exemptions in the UK Data Protection Laws
   1. The Importer is not required to respond to requests or provide information or notifications under Sections 18, 19, 20, 21 and 23 if:
      1. it is unable to reasonably verify the identity of an individual making the request; or
      2. the requests are manifestly unfounded or excessive, including where requests are repetitive. In that case the Importer may refuse the request or may charge the Relevant Data Subject a reasonable fee; or
      3. a relevant exemption would be available under UK Data Protection Laws, were the Importer subject to the UK Data Protection Laws.

If the Importer refuses an individual’s request or charges a fee under Section 22.1.2 it will set out in writing the reasons for its refusal or charge, and inform the Relevant Data Subject that they are entitled to bring a claim for compensation under this IDTA in the case of any breach of this IDTA.

**How to give third parties access to Transferred Data under Local Laws**

1. Access requests and direct access
   1. In this Section ‎23 an “Access Request” is a legally binding request (except for requests only binding by contract law) to access any Transferred Data and “Direct Access” means direct access to any Transferred Data by public authorities of which the Importer is aware.
   2. The Importer may disclose any requested Transferred Data in so far as it receives an Access Request, unless in the circumstances it is reasonable for it to challenge that Access Request on the basis there are significant grounds to believe that it is unlawful.
   3. In so far as Local Laws allow and it is reasonable to do so, the Importer will Without Undue Delay provide the following with relevant information about any Access Request or Direct Access: the Exporter; any Third Party Controller; and where the Importer is a Controller, any Relevant Data Subjects.
   4. In so far as Local Laws allow, the Importer must:
      1. make and keep a written record of Access Requests and Direct Access, including (if known): the dates, the identity of the requestor/accessor, the purpose of the Access Request or Direct Access, the type of data requested or accessed, whether it was challenged or appealed, and the outcome; and the Transferred Data which was provided or accessed; and
      2. provide a copy of this written record to the Exporter on each Review Date and any time the Exporter or the ICO reasonably requests.
2. Giving notice
   1. If a Party is required to notify any other Party in this IDTA it will be marked for the attention of the relevant Key Contact and sent by e-mail to the e-mail address given for the Key Contact.
   2. If the notice is sent in accordance with Section 24.1, it will be deemed to have been delivered at the time the e-mail was sent, or if that time is outside of the receiving Party’s normal business hours, the receiving Party’s next normal business day, and provided no notice of non-delivery or bounceback is received.
   3. The Parties agree that any Party can update their Key Contact details by giving 14 days’ (or more) notice in writing to the other Party.
3. General clauses
   1. In relation to the transfer of the Transferred Data to the Importer and the Importer’s Processing of the Transferred Data, this IDTA and any Linked Agreement:
      1. contain all the terms and conditions agreed by the Parties; and
      2. override all previous contacts and arrangements, whether oral or in writing.
   2. If one Party made any oral or written statements to the other before entering into this IDTA (which are not written in this IDTA) the other Party confirms that it has not relied on those statements and that it will not have a legal remedy if those statements are untrue or incorrect, unless the statement was made fraudulently.
   3. Neither Party may novate, assign or obtain a legal charge over this IDTA (in whole or in part) without the written consent of the other Party, which may be set out in the Linked Agreement.
   4. Except as set out in Section 17.1, neither Party may sub contract its obligations under this IDTA without the written consent of the other Party, which may be set out in the Linked Agreement.
   5. This IDTA does not make the Parties a partnership, nor appoint one Party to act as the agent of the other Party.
   6. If any Section (or part of a Section) of this IDTA is or becomes illegal, invalid or unenforceable, that will not affect the legality, validity and enforceability of any other Section (or the rest of that Section) of this IDTA.
   7. If a Party does not enforce, or delays enforcing, its rights or remedies under or in relation to this IDTA, this will not be a waiver of those rights or remedies. In addition, it will not restrict that Party’s ability to enforce those or any other right or remedy in future.
   8. If a Party chooses to waive enforcing a right or remedy under or in relation to this IDTA, then this waiver will only be effective if it is made in writing. Where a Party provides such a written waiver:
      1. it only applies in so far as it explicitly waives specific rights or remedies;
      2. it shall not prevent that Party from exercising those rights or remedies in the future (unless it has explicitly waived its ability to do so); and
      3. it will not prevent that Party from enforcing any other right or remedy in future.

**What happens if there is a breach of this IDTA?**

1. Breaches of this IDTA
   1. Each Party must notify the other Party in writing (and with all relevant details) if it:
      1. has breached this IDTA; or
      2. it should reasonably anticipate that it may breach this IDTA, and provide any information about this which the other Party reasonably requests.
   2. In this IDTA “Significant Harmful Impact” means that there is more than a minimal risk of a breach of the IDTA causing (directly or indirectly) significant damage to any Relevant Data Subject or the other Party.
2. Breaches of this IDTA by the Importer
   1. If the Importer has breached this IDTA, and this has a Significant Harmful Impact, the Importer must take steps Without Undue Delay to end the Significant Harmful Impact, and if that is not possible to reduce the Significant Harmful Impact as much as possible.
   2. Until there is no ongoing Significant Harmful Impact on Relevant Data Subjects:
      1. the Exporter must suspend sending Transferred Data to the Importer;
      2. If the Importer is the Exporter’s Processor or Sub-Processor: if the Exporter requests, the importer must securely delete all Transferred Data or securely return it to the Exporter (or a third party named by the Exporter); and
      3. if the Importer has transferred on the Transferred Data to a third party receiver under Section 16, and the breach has a Significant Harmful Impact on Relevant Data Subject when it is Processed by or on behalf of that third party receiver, the Importer must:
         1. notify the third party receiver of the breach and suspend sending it Transferred Data; and
         2. if the third party receiver is the Importer’s Processor or Sub-Processor: make the third party receiver securely delete all Transferred Data being Processed by it or on its behalf, or securely return it to the Importer (or a third party named by the Importer).
   3. If the breach cannot be corrected Without Undue Delay, so there is no ongoing Significant Harmful Impact on Relevant Data Subjects, the Exporter must end this IDTA under Section 30.1.
3. Breaches of this IDTA by the Exporter
   1. If the Exporter has breached this IDTA, and this has a Significant Harmful Impact, the Exporter must take steps Without Undue Delay to end the Significant Harmful Impact and if that is not possible to reduce the Significant Harmful Impact as much as possible.
   2. Until there is no ongoing risk of a Significant Harmful Impact on Relevant Data Subjects, the Exporter must suspend sending Transferred Data to the Importer.
   3. If the breach cannot be corrected Without Undue Delay, so there is no ongoing Significant Harmful Impact on Relevant Data Subjects, the Importer must end this IDTA under Section 30.1.

**Ending the IDTA**

1. How to end this IDTA without there being a breach
   1. The IDTA will end:
      1. at the end of the Term stated in Table 2: Transfer Details; or
      2. if in Table 2: Transfer Details, the Parties can end this IDTA by providing written notice to the other: at the end of the notice period stated;
      3. at any time that the Parties agree in writing that it will end; or
      4. at the time set out in Section 29.2.
   2. If the ICO issues a revised Approved IDTA under Section 5.4, if any Party selected in Table 2 “Ending the IDTA when the Approved IDTA changes”, will as a direct result of the changes in the Approved IDTA have a substantial, disproportionate and demonstrable increase in:
      1. its direct costs of performing its obligations under the IDTA; and/or
      2. its risk under the IDTA,

and in either case it has first taken reasonable steps to reduce that cost or risk so that it is not substantial and disproportionate, that Party may end the IDTA at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved IDTA.

1. How to end this IDTA if there is a breach
   1. A Party may end this IDTA immediately by giving the other Party written notice if:
      1. the other Party has breached this IDTA and this has a Significant Harmful Impact. This includes repeated minor breaches which taken together have a Significant Harmful Impact, and
         1. the breach can be corrected so there is no Significant Harmful Impact, and the other Party has failed to do so Without Undue Delay (which cannot be more than 14 days of being required to do so in writing); or
         2. the breach and its Significant Harmful Impact cannot be corrected;
      2. the Importer can no longer comply with Section 8.3, as there are Local Laws which mean it cannot comply with this IDTA and this has a Significant Harmful Impact.
2. What must the Parties do when the IDTA ends?
   1. If the parties wish to bring this IDTA to an end or this IDTA ends in accordance with any provision in this IDTA, but the Importer must comply with a Local Law which requires it to continue to keep any Transferred Data then this IDTA will remain in force in respect of any retained Transferred Data for as long as the retained Transferred Data is retained, and the Importer must:
      1. notify the Exporter Without Undue Delay, including details of the relevant Local Law and the required retention period;
      2. retain only the minimum amount of Transferred Data it needs to comply with that Local Law, and the Parties must ensure they maintain the Appropriate Safeguards, and change the Tables and Extra Protection Clauses, together with any TRA to reflect this; and
      3. stop Processing the Transferred Data as soon as permitted by that Local Law and the IDTA will then end and the rest of this Section 31 will apply.
   2. When this IDTA ends (no matter what the reason is):
      1. the Exporter must stop sending Transferred Data to the Importer; and
      2. if the Importer is the Exporter’s Processor or Sub-Processor: the Importer must delete all Transferred Data or securely return it to the Exporter (or a third party named by the Exporter), as instructed by the Exporter;
      3. if the Importer is a Controller and/or not the Exporter’s Processor or Sub-Processor: the Importer must securely delete all Transferred Data.
      4. the following provisions will continue in force after this IDTA ends (no matter what the reason is):
3. Section 1 (This IDTA and Linked Agreements);
4. Section 2 (Legal Meaning of Words);
5. Section 6 (Understanding this IDTA);
6. Section 7 (Which laws apply to this IDTA);
7. Section 10 (The ICO);
8. Sections 11.1 and 11.4 (Exporter’s obligations);
9. Sections 12.1.2, 12.1.3, 12.1.4, 12.1.5 and 12.1.6 (General Importer obligations);
10. Section 13.1 (Importer’s obligations if it is subject to UK Data Protection Laws);
11. Section 17 (*Importer’s responsibility if it authorised others to perform its obligations*);
12. Section 24 (*Giving notice*);
13. Section 25 (*General clauses*);
14. Section 31 (*What must the Parties do when the IDTA ends*);
15. Section 32 (*Your liability*);
16. Section 33 (*How Relevant Data Subjects and the ICO may bring legal claims*);
17. Section 34 (*Courts legal claims can be brought in*);
18. Section 35 (*Arbitration*); and
19. Section 36 (*Legal Glossary*).

**How to bring a legal claim under this IDTA**

1. Your liability
   1. The Parties remain fully liable to Relevant Data Subjects for fulfilling their obligations under this IDTA and (if they apply) under UK Data Protection Laws.
   2. Each Party (in this Section, “Party One”) agrees to be fully liable to Relevant Data Subjects for the entire damage suffered by the Relevant Data Subject, caused directly or indirectly by:
      1. Party One’s breach of this IDTA; and/or
      2. where Party One is a Processor, Party One’s breach of any provisions regarding its Processing of the Transferred Data in the Linked Agreement;
      3. where Party One is a Controller, a breach of this IDTA by the other Party if it involves Party One’s Processing of the Transferred Data (no matter how minimal)

in each case unless Party One can prove it is not in any way responsible for the event giving rise to the damage.

* 1. If one Party has paid compensation to a Relevant Data Subject under Section 32.2, it is entitled to claim back from the other Party that part of the compensation corresponding to the other Party’s responsibility for the damage, so that the compensation is fairly divided between the Parties.
  2. The Parties do not exclude or restrict their liability under this IDTA or UK Data Protection Laws, on the basis that they have authorised anyone who is not a Party (including a Processor) to perform any of their obligations, and they will remain responsible for performing those obligations.

1. How Relevant Data Subjects and the ICO may bring legal claims
   1. The Relevant Data Subjects are entitled to bring claims against the Exporter and/or Importer for breach of the following (including where their Processing of the Transferred Data is involved in a breach of the following by either Party):
2. Section 1 (*This IDTA and Linked Agreements*);
3. Section 3 (*You have provided all the information required by Part one: Tables and Part two: Extra Protection Clauses*);
4. Section 8 (*The Appropriate Safeguards*);
5. Section 9 (*Reviews to ensure the Appropriate Safeguards continue*);
6. Section 11 (*Exporter’s obligations*);
7. Section 12 (*General Importer Obligations*);
8. Section 13 (*Importer’s obligations if it is subject to UK Data Protection Laws*);
9. Section 14 (*Importer’s obligations to comply with key data protection laws*);
10. Section 15 (*What happens if there is an Importer Personal Data Breach*);
11. Section 16 (*Transferring on the Transferred Data*);
12. Section 17 (*Importer’s responsibility if it authorises others to perform its obligations*);
13. Section 18 (*The right to a copy of the IDTA*);
14. Section 19 (*The Importer’s contact details for the Relevant Data Subjects*);
15. Section 20 (*How Relevant Data Subjects can exercise their data subject rights*);
16. Section 21 (*How Relevant Data Subjects can exercise their data subject rights– if the Importer is the Exporter’s Processor or Sub-Processor*);
17. Section 23 (*Access Requests and Direct Access*);
18. Section 26 (*Breaches of this IDTA*);
19. Section 27 (*Breaches of this IDTA by the Importer*);
20. Section 28 (*Breaches of this IDTA by the Exporter*);
21. Section 30 (*How to end this IDTA if there is a breach*);
22. Section 31 (*What must the Parties do when the IDTA ends*); and
23. any other provision of the IDTA which expressly or by implication benefits the Relevant Data Subjects.
    1. The ICO is entitled to bring claims against the Exporter and/or Importer for breach of the following Sections: Section 10 (*The ICO*), Sections 11.1 and 11.2 (*Exporter’s obligations*), Section 12.1.6 (*General Importer obligations*) and Section 13 (*Importer’s obligations if it is subject to UK Data Protection Laws*).
    2. No one else (who is not a Party) can enforce any part of this IDTA (including under the Contracts (Rights of Third Parties) Act 1999).
    3. The Parties do not need the consent of any Relevant Data Subject or the ICO to make changes to this IDTA, but any changes must be made in accordance with its terms.
    4. In bringing a claim under this IDTA, a Relevant Data Subject may be represented by a not-for-profit body, organisation or association under the same conditions set out in Article 80(1) UK GDPR and sections 187 to 190 of the Data Protection Act 2018.
24. Courts legal claims can be brought in
    1. The courts of the UK country set out in Table 2: Transfer Details have non-exclusive jurisdiction over any claim in connection with this IDTA (including non-contractual claims).
    2. The Exporter may bring a claim against the Importer in connection with this IDTA (including non-contractual claims) in any court in any country with jurisdiction to hear the claim.
    3. The Importer may only bring a claim against the Exporter in connection with this IDTA (including non-contractual claims) in the courts of the UK country set out in the Table 2: Transfer Details
    4. Relevant Data Subjects and the ICO may bring a claim against the Exporter and/or the Importer in connection with this IDTA (including non-contractual claims) in any court in any country with jurisdiction to hear the claim.
    5. Each Party agrees to provide to the other Party reasonable updates about any claims or complaints brought against it by a Relevant Data Subject or the ICO in connection with the Transferred Data (including claims in arbitration).
25. Arbitration
    1. Instead of bringing a claim in a court under Section 34, any Party, or a Relevant Data Subject may elect to refer any dispute arising out of or in connection with this IDTA (including non-contractual claims) to final resolution by arbitration under the Rules of the London Court of International Arbitration, and those Rules are deemed to be incorporated by reference into this Section ‎35.
    2. The Parties agree to submit to any arbitration started by another Party or by a Relevant Data Subject in accordance with this Section ‎‎35.
    3. There must be only one arbitrator. The arbitrator (1) must be a lawyer qualified to practice law in one or more of England and Wales, or Scotland, or Northern Ireland and (2) must have experience of acting or advising on disputes relating to UK Data Protection Laws.
    4. London shall be the seat or legal place of arbitration. It does not matter if the Parties selected a different UK country as the ‘primary place for legal claims to be made’ in Table 2: Transfer Details.
    5. The English language must be used in the arbitral proceedings.
    6. English law governs this Section ‎‎35. This applies regardless of whether or not the parties selected a different UK country’s law as the ‘UK country’s law that governs the IDTA’ in Table 2: Transfer Details.
26. Legal Glossary

| Word or Phrase | Legal definition (this is how this word or phrase must be interpreted in the IDTA) |
| --- | --- |
| **Access Request** | As defined in Section 23, as a legally binding request (except for requests only binding by contract law) to access any Transferred Data. |
| **Adequate Country** | A third country, or:   1. a territory; 2. one or more sectors or organisations within a third country; 3. an international organisation;   which the Secretary of State has specified by regulations provides an adequate level of protection of Personal Data in accordance with Section 17A of the Data Protection Act 2018. |
| **Appropriate Safeguards** | The standard of protection over the Transferred Data and of the Relevant Data Subject’s rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR. |
| **Approved IDTA** | The template IDTA A1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 5.4. |
| **Commercial Clauses** | The commercial clauses set out in Part three. |
| **Controller** | As defined in the UK GDPR. |
| **Damage** | All material and non-material loss and damage. |
| **Data Subject** | As defined in the UK GDPR. |
| **Decision-Making** | As defined in Section 20.6, as decisions about the Relevant Data Subjects based solely on automated processing, including profiling, using the Transferred Data. |
| **Direct Access** | As defined in Section 23 as direct access to any Transferred Data by public authorities of which the Importer is aware. |
| **Exporter** | The exporter identified in Table 1: Parties & Signature. |
| **Extra Protection Clauses** | The clauses set out in Part two: Extra Protection Clauses. |
| **ICO** | The Information Commissioner. |
| **Importer** | The importer identified in Table 1: Parties & Signature. |
| **Importer Data Subject Contact** | The Importer Data Subject Contact identified in Table 1: Parties & Signature, which may be updated in accordance with Section 19. |
| **Importer Information** | As defined in Section 8.3.1, as all relevant information regarding Local Laws and practices and the protections and risks which apply to the Transferred Data when it is Processed by the Importer, including for the Exporter to carry out any TRA. |
| **Importer Personal Data Breach** | A ‘personal data breach’ as defined in UK GDPR, in relation to the Transferred Data when Processed by the Importer. |
| **Linked Agreement** | The linked agreements set out in Table 2: Transfer Details (if any). |
| **Local Laws** | Laws which are not the laws of the UK and which bind the Importer. |
| **Mandatory Clauses** | Part four: Mandatory Clauses of this IDTA. |
| **Notice Period** | As set out in Table 2: Transfer Details. |
| **Party/Parties** | The parties to this IDTA as set out in Table 1: Parties & Signature. |
| **Personal Data** | As defined in the UK GDPR. |
| **Personal Data Breach** | As defined in the UK GDPR. |
| **Processing** | As defined in the UK GDPR.  When the IDTA refers to Processing by the Importer, this includes where a third party Sub-Processor of the Importer is Processing on the Importer’s behalf. |
| **Processor** | As defined in the UK GDPR. |
| **Purpose** | The ‘Purpose’ set out in Table 2: Transfer Details, including any purposes which are not incompatible with the purposes stated or referred to. |
| **Relevant Data Subject** | A Data Subject of the Transferred Data. |
| **Restricted Transfer** | A transfer which is covered by Chapter V of the UK GDPR |
| **Review Dates** | The review dates or period for the Security Requirements set out in Table 2: Transfer Details, and any review dates set out in any revised Approved IDTA. |
| **Significant Harmful Impact** | As defined in Section 26.2 as where there is more than a minimal risk of the breach causing (directly or indirectly) significant harm to any Relevant Data Subject or the other Party. |
| **Special Category Data** | As described in the UK GDPR, together with criminal conviction or criminal offence data. |
| **Start Date** | As set out in Table 1: Parties and signature. |
| **Sub-Processor** | A Processor appointed by another Processor to Process Personal Data on its behalf.  This includes Sub-Processors of any level, for example a Sub-Sub-Processor. |
| **Tables** | The Tables set out in Part one of this IDTA. |
| **Term** | As set out in Table 2: Transfer Details. |
| **Third Party Controller** | The Controller of the Transferred Data where the Exporter is a Processor or Sub-Processor  If there is not a Third Party Controller this can be disregarded. |
| **Transfer Risk Assessment or TRA** | A risk assessment in so far as it is required by UK Data Protection Laws to demonstrate that the IDTA provides the Appropriate Safeguards |
| **Transferred Data** | Any Personal Data which the Parties transfer, or intend to transfer under this IDTA, as described in Table 2: Transfer Details |
| **UK Data Protection Laws** | All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018. |
| **UK GDPR** | As defined in Section 3 of the Data Protection Act 2018. |
| **Without Undue Delay** | Without undue delay, as that phase is interpreted in the UK GDPR. |

**Alternative Part 4 Mandatory Clauses:**

|  |  |
| --- | --- |
| **Mandatory Clauses** | Part 4: Mandatory Clauses of the Approved IDTA, being the template IDTA A.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section ‎5.4 of those Mandatory Clauses. |

## Part B: International Data Transfer Agreement Addendum to the EU Commission Standard Contractual Clauses



Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

**VERSION B1.0, in force 21 March 2022**

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

### Part 1: Tables

**Table 1: Parties**

|  |  |
| --- | --- |
| **Start date** |  |
|  |  |

| The Parties | Exporter (who sends the Restricted Transfer) | Importer (who receives the Restricted Transfer) |
| --- | --- | --- |
| **Parties’ details** | Full legal name:  Trading name (if different):  Main address (if a company registered address):  Official registration number (if any) (company number or similar identifier): | Full legal name:  Trading name (if different):  Main address (if a company registered address):  Official registration number (if any) (company number or similar identifier): |
| **Key Contact** | Full Name (optional):  Job Title:  Contact details including email: | Full Name (optional):  Job Title:  Contact details including email: |
| **Signature (if required for the purposes of Section ‎2)** |  |  |

**Table 2: Selected SCCs, Modules and Selected Clauses**

|  |  |
| --- | --- |
| **Addendum EU SCCs** | The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:  Date:  Reference (if any):  Other identifier (if any):  Or  the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum: |

| Module | Module in operation | Clause 7 (Docking Clause) | Clause 11  (Option) | Clause 9a (Prior Authorisation or General Authorisation) | Clause 9a (Time period) | Is personal data received from the Importer combined with personal data collected by the Exporter? |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**Table 3: Appendix Information**

“**Appendix Information**” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

|  |
| --- |
| Annex 1A: List of Parties: |
| Annex 1B: Description of Transfer: |
| Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: |
| Annex III: List of Sub processors (Modules 2 and 3 only): |

**Table 4: Ending this Addendum when the Approved Addendum Changes**

|  |  |
| --- | --- |
| **Ending this Addendum when the Approved Addendum changes** | Which Parties may end this Addendum as set out in Section 19:  Importer  Exporter  neither Party |

### Part 2: Mandatory Clauses

**Entering into this Addendum**

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

**Interpretation of this Addendum**

1. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

|  |  |
| --- | --- |
| **Addendum** | This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs. |
| **Addendum EU SCCs** | The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information. |
| **Appendix Information** | As set out in Table 3. |
| **Appropriate Safeguards** | The standard of protection over the personal data and of data subjects’ rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR. |
| **Approved Addendum** | The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18. |
| **Approved EU SCCs** | The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021. |
| **ICO** | The Information Commissioner. |
| **Restricted Transfer** | A transfer which is covered by Chapter V of the UK GDPR. |
| **UK** | The United Kingdom of Great Britain and Northern Ireland. |
| **UK Data Protection Laws** | All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018. |
| **UK GDPR** | As defined in section 3 of the Data Protection Act 2018. |

1. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties’ obligation to provide the Appropriate Safeguards.
2. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.
3. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.
4. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
5. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

**Hierarchy**

1. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.
2. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.
3. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

**Incorporation of and changes to the EU SCCs**

1. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
   * + 1. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter’s processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
       2. Sections 9 to 11 override Clause 5 (*Hierarchy*) of the Addendum EU SCCs; and
       3. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.
2. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.
3. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.
4. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:
   * + 1. References to the “Clauses” means this Addendum, incorporating the Addendum EU SCCs;
       2. In Clause 2, delete the words:

“and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679”;

* + - 1. Clause 6 (Description of the transfer(s)) is replaced with:

“The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter’s processing when making that transfer.”;

* + - 1. Clause 8.7(i) of Module 1 is replaced with:

“it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer”;

* + - 1. Clause 8.8(i) of Modules 2 and 3 is replaced with:

“the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;”

* + - 1. References to “Regulation (EU) 2016/679”, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)” and “that Regulation” are all replaced by “UK Data Protection Laws”. References to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws;
      2. References to Regulation (EU) 2018/1725 are removed;
      3. References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;
      4. The reference to “Clause 12(c)(i)” at Clause 10(b)(i) of Module one, is replaced with “Clause 11(c)(i)”;
      5. Clause 13(a) and Part C of Annex I are not used;
      6. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;
      7. In Clause 16(e), subsection (i) is replaced with:

“the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”;

* + - 1. Clause 17 is replaced with:

“These Clauses are governed by the laws of England and Wales.”;

* + - 1. Clause 18 is replaced with:

“Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and

* + - 1. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

**Amendments to this Addendum**

1. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.
2. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
3. From time to time, the ICO may issue a revised Approved Addendum which:
   * + 1. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
       2. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

1. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:
   * + 1. its direct costs of performing its obligations under the Addendum; and/or
       2. its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

1. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

### Alternative Part 2 Mandatory Clauses:

|  |  |
| --- | --- |
| **Mandatory Clauses** | Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section ‎18 of those Mandatory Clauses. |

## Annex 3: Standard Contractual Clauses for EU GDPR Compliant Transfers

***[Guidance: Delete this Annex and replace with the text ‘NOT USED’ if the Authority has chosen to refer out to the IDTA, rather than incorporating the text, that is, by selecting the first set of square brackets in Clause 21 of the Core Terms and in this Schedule.]***

## Part A: Processor to Controller Standard Contractual Clauses

#### Standard Contractual Clauses for Personal Data Transfers from an EU Processor to a Controller Established in a Third Country (Processor-to-Controller Transfers)

**SECTION I**

**CLAUSE 1**

**Purpose and scope**

* + - 1. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[[FN1](#bookmark=id.2coe5ab)] for the transfer of personal data to a third country.
      2. The Parties:
         1. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and
         2. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

* + - 1. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
      2. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

**CLAUSE 2**

**Effect and invariability of the Clauses**

* + - 1. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
      2. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

**CLAUSE 3**

**Third-party beneficiaries**

* + - 1. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
         1. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
         2. Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
         3. Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
         4. Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
         5. Clause 13;
         6. Clause 15.1(c), (d) and (e);
         7. Clause 16(e);
         8. Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.
      2. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

**CLAUSE 4**

**Interpretation**

* + - 1. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
      2. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
      3. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

**CLAUSE 5**

**Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

**CLAUSE 6**

**Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

**[CLAUSE 7 - Optional**

**Docking clause**

* + - 1. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
      2. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
      3. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.]

**SECTION II – OBLIGATIONS OF THE PARTIES**

**CLAUSE 8**

**Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

**8.1 Instructions**

* + - 1. The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.
      2. The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.
      3. The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.
      4. After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

**8.2 Security of processing**

* + - 1. The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data[[FN7](#bookmark=id.rtofi4)], the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.
      2. The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph 8.2(a)‎. In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.
      3. The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

**8.3 Documentation and compliance**

* 1. The Parties shall be able to demonstrate compliance with these Clauses.
  2. The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

**CLAUSE 9**

**Use of sub-processors**

N/A

**CLAUSE 10**

**Data subject rights**

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

**CLAUSE 11**

**Redress**

* + - 1. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[**OPTION**: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body[[FN11](#bookmark=id.3btby5x)] at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a)‎, of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

**CLAUSE 12**

**Liability**

* + - 1. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
      2. Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.
      3. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
      4. The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
      5. The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

**CLAUSE 13**

**Supervision**

N/A

**SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

**CLAUSE 14**

**Local laws and practices affecting compliance with the Clauses** *(where the EU processor combines the personal data received from the third country-controller with personal data collected by the* processor *in the EU)*

* + - 1. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
      2. The Parties declare that in providing the warranty in paragraph ‎(a), they have taken due account in particular of the following elements:
    1. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
    2. the laws and practices of the third country of destination – including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[[FN12](#bookmark=id.1qym8dq)];
    3. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
       1. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
       2. The Parties agree to document the assessment under paragraph ‎(b) and make it available to the competent supervisory authority on request.
       3. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a)‎.
       4. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and 16(e) shall apply.

**CLAUSE 15**

**Obligations of the data importer in case of access by public authorities** *(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

**15.1 Notification**

* + - 1. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
    1. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
    2. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
       1. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
       2. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
       3. The data importer agrees to preserve the information pursuant to paragraphs ‎(a)‎ to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
       4. Paragraphs (a)‎ to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

**15.2 Review of legality and data minimisation**

* + - 1. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
      2. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
      3. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

**SECTION IV – FINAL PROVISIONS**

**CLAUSE** **16**

**Non-compliance with the Clauses and termination**

* + - 1. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
      2. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
      3. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
    1. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b)‎ and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
    2. the data importer is in substantial or persistent breach of these Clauses; or
    3. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

* + - 1. Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
      2. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

**CLAUSE 17**

**Governing law**

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of \_\_\_\_\_\_\_ (*specify country*).

**CLAUSE 18**

**Choice of forum and jurisdiction**

Any dispute arising from these Clauses shall be resolved by the courts of \_\_\_\_\_ (*specify country*).

**Official European Commission Footnotes**

[FN1](#bookmark=id.1l354xk): Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

[FN7](#bookmark=id.2zlqixl): This includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.

[FN11](#bookmark=id.25lcl3g): The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

[FN12](#bookmark=id.3vkm5x4): As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

**APPENDIX**

|  |
| --- |
| EXPLANATORY NOTE:  It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used. |

**ANNEX** **I**

**A. LIST OF PARTIES**

**Data exporter(s):** [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

1. Name: …………………….

Address: …………………….

Contact person's name, position and contact details: ……………...…

Activities relevant to the data transferred under these Clauses: …..…

Signature and date: ………………….…

Role (controller/processor): ……………………..…

2. …

**Data importer(s):** [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*]

1. Name: …………………….

Address: …………………….

Contact person's name, position and contact details: ……………...…

Activities relevant to the data transferred under these Clauses: …..…

Signature and date: ………………….…

Role (controller/processor): ……………………..…

2. …

**B. DESCRIPTION OF TRANSFER**

*Categories of data subjects whose personal data is transferred*

*……………………………..*

*Categories of personal data transferred*

*……………………………..*

*Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.*

*……………………………..*

*The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).*

*……………………………..*

*Nature of the processing*

*……………………………..*

*Purpose(s) of the data transfer and further processing*

*……………………………..*

*The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*

*……………………………..*

*For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing*

*……………………………..*

## Part B: Controller to Processor Standard Contractual Clauses

**Standard Contractual Clauses for Personal Data Transfers from an EU Controller to a Processor Established in a Third Country (Controller-to-Processor Transfers)**

**SECTION I**

**CLAUSE 1**

**Purpose and scope**

* 1. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[[FN1](#bookmark=id.1qhz01q)] for the transfer of personal data to a third country.
  2. The Parties:
     1. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and
     2. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

* 1. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
  2. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

**CLAUSE 2**

**Effect and invariability of the Clauses**

* 1. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
  2. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

**CLAUSE 3**

**Third-party beneficiaries**

* 1. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
     1. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
     2. Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
     3. Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
     4. Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
     5. Clause 13;
     6. Clause 15.1(c), (d) and (e);
     7. Clause 16(e);
     8. Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.
  2. Paragraph ‎(a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

**CLAUSE 4**

**Interpretation**

* 1. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
  2. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
  3. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

**CLAUSE 5**

**Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

**CLAUSE 6**

**Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

**[Optional: CLAUSE 7**

**Docking clause**

* 1. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
  2. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
  3. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.]

**SECTION II – OBLIGATIONS OF THE PARTIES**

**CLAUSE 8**

**Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

**8.1 Instructions**

* 1. The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
  2. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

**8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

**8.3 Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

**8.4 Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

**8.5 Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

**8.6 Security of processing**

* 1. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
  2. The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
  3. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
  4. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

**8.7 Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

**8.8 Onward transfers**

* 1. The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[[FN4](#bookmark=id.4ahmipj)] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:
     1. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
     2. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
     3. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
     4. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.
  2. Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

**8.9 Documentation and compliance**

* 1. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
  2. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
  3. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
  4. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
  5. The Parties shall make the information referred to in paragraphs ‎(b) and (c), including the results of any audits, available to the competent supervisory authority on request.

**CLAUSE 9**

**Use of sub-processors**

OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least [*Specify time period*] prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*Specify time period*] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

* 1. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. [[FN8](#bookmark=id.2pmwsxc)] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
  2. The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
  3. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
  4. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

**CLAUSE 10**

**Data subject rights**

* 1. The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
  2. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
  3. In fulfilling its obligations under paragraphs ‎(a) and (b), the data importer shall comply with the instructions from the data exporter.

**CLAUSE 11**

**Redress**

* 1. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[**Optional**: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body[[FN11](#bookmark=id.14s7355)] at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a)‎, of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

* 1. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
  2. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
     1. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
     2. refer the dispute to the competent courts within the meaning of Clause 18.
  3. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
  4. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
  5. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

**CLAUSE 12**

**Liability**

* 1. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
  2. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
  3. Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
  4. The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
  5. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
  6. The Parties agree that if one Party is held liable under paragraph ‎(e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
  7. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

**CLAUSE 13**

**Supervision**

* 1. [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

* 1. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

**SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

**CLAUSE** **14**

**Local laws and practices affecting compliance with the Clauses**

* 1. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
  2. The Parties declare that in providing the warranty in paragraph ‎(a), they have taken due account in particular of the following elements:
     1. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
     2. the laws and practices of the third country of destination – including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[[FN12](#bookmark=id.3orulsy)];
     3. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
  3. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
  4. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
  5. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph ‎(a).
  6. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

**CLAUSE 15**

**Obligations of the data importer in case of access by public authorities**

**15.1 Notification**

* 1. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
     1. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
     2. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
  2. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
  3. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
  4. The data importer agrees to preserve the information pursuant to paragraphs ‎(a) to ‎(c) for the duration of the contract and make it available to the competent supervisory authority on request.
  5. Paragraphs (a) to ‎(c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

**15.2 Review of legality and data minimisation**

* 1. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
  2. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
  3. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

**SECTION IV – FINAL PROVISIONS**

**CLAUSE 16**

**Non-compliance with the Clauses and termination**

* 1. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
  2. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
  3. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
     1. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph(b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
     2. the data importer is in substantial or persistent breach of these Clauses; or
     3. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

* 1. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph ‎(c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
  2. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

**CLAUSE 17**

**Governing law**

[OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of \_\_\_\_\_\_\_ (*specify Member State*).]

[OPTION 2: These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of \_\_\_\_\_\_\_ (*specify Member State*).]

**CLAUSE 18**

**Choice of forum and jurisdiction**

* 1. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
  2. The Parties agree that those shall be the courts of \_\_\_\_\_ *(specify Member State)*.
  3. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
  4. The Parties agree to submit themselves to the jurisdiction of such courts.

**Official European Commission Footnotes**

[FN1](#bookmark=id.1l354xk): Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

[FN4](#bookmark=id.2367nm2): The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union’s internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[FN8](#bookmark=id.ng1svc): This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[FN11](#bookmark=id.3qg2avn): The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

[FN12](#bookmark=id.3v3yxl4): As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

**APPENDIX**

|  |
| --- |
| EXPLANATORY NOTE:  It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used. |

**ANNEX** **I**

**A. LIST OF PARTIES**

**Data exporter(s):** [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

1. Name: …………………….

Address: …………………….

Contact person's name, position and contact details: ……………...…

Activities relevant to the data transferred under these Clauses: …..…

Signature and date: ………………….…

Role (controller/processor): ……………………..…

2. …

**Data importer(s):** [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*]

1. Name: …………………….

Address: …………………….

Contact person's name, position and contact details: ……………...…

Activities relevant to the data transferred under these Clauses: …..…

Signature and date: ………………….…

Role (controller/processor): ……………………..…

2. …

**B. DESCRIPTION OF TRANSFER**

*Categories of data subjects whose personal data is transferred*

*………………….*

*Categories of personal data transferred*

*………………….*

*Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.*

*………………….*

*The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).*

*………………….*

*Nature of the processing*

*………………….*

*Purpose(s) of the data transfer and further processing*

*………………….*

*The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*

*………………….*

*For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing*

*………………….*

**C. COMPETENT SUPERVISORY AUTHORITY**

*Identify the competent supervisory authority/ies in accordance with Clause 13.*

**ANNEX** **II**

**TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

|  |
| --- |
| EXPLANATORY NOTE:  The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers. |

*Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.*

*[Examples of possible measures:*

*Measures of pseudonymisation and encryption of personal data*

*Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services*

*Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident*

*Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing*

*Measures for user identification and authorisation*

*Measures for the protection of data during transmission*

*Measures for the protection of data during storage*

*Measures for ensuring physical security of locations at which personal data are processed*

*Measures for ensuring events logging*

*Measures for ensuring system configuration, including default configuration*

*Measures for internal IT and IT security governance and management*

*Measures for certification/assurance of processes and products*

*Measures for ensuring data minimisation*

*Measures for ensuring data quality*

*Measures for ensuring limited data retention*

*Measures for ensuring accountability*

*Measures for allowing data portability and ensuring erasure]*

*For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the* *controller and, for transfers from a processor to a sub-processor, to the data exporter*

**ANNEX** **III**

**LIST OF SUB-PROCESSORS**

|  |
| --- |
| EXPLANATORY NOTE:  This Annex must be completed in case of the specific authorization of sub-processors (Clause 9(a), Option 1). |

The controller has authorised the use of the following sub-processors:

1. Name: ………………………

Address: ……………………

Contact person's name, position and contact details: …………………………..….

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): …………………………………..

2. ……..

## Part C: Processor to Processor Standard Contractual Clauses

**Standard Contractual Clauses for Personal Data Transfers from an EU Processor to a Processor Established in a Third Country (Processor-to-Processor Transfers)**

**SECTION I**

**CLAUSE 1**

**Purpose and scope**

* 1. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[[FN1](#bookmark=id.32lfgkd)] for the transfer of personal data to a third country.
  2. The Parties:
     1. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and
     2. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

* 1. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
  2. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

**CLAUSE 2**

**Effect and invariability of the Clauses**

* 1. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
  2. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

**CLAUSE 3**

**Third-party beneficiaries**

* 1. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
     1. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
     2. Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
     3. Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
     4. Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
     5. Clause 13;
     6. Clause 15.1(c), (d) and (e);
     7. Clause 16(e);
     8. Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.
  2. Paragraph (a)‎ is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

**CLAUSE 4**

**Interpretation**

* 1. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
  2. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
  3. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

**CLAUSE 5**

**Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

**CLAUSE 6**

**Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

**[CLAUSE 7 - Optional**

**Docking clause**

* 1. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
  2. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
  3. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.]

**SECTION II - OBLIGATIONS OF THE PARTIES**

**CLAUSE 8**

**Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

**8.1 Instructions**

* 1. The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.
  2. The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.
  3. The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.
  4. The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter[[FN5](#bookmark=id.1hqpqs6)].

**8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

**8.3 Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

**8.4 Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

**8.5 Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

**8.6 Security of processing**

* 1. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
  2. The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
  3. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
  4. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

**8.7 Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

**8.8 Onward transfers**

* 1. The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[[FN6](#bookmark=id.41qd9fz)] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:
     1. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
     2. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;
     3. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
     4. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.
  2. Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

**8.9 Documentation and compliance**

* 1. The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.
  2. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.
  3. The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.
  4. The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.
  5. Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.
  6. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
  7. The Parties shall make the information referred to in paragraphs ‎(b) and (c), including the results of any audits, available to the competent supervisory authority on request.

**CLAUSE 9**

**Use of sub-processors**

OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the prior specific written authorisation of the controller. The data importer shall submit the request for specific authorisation at least [*Specify time period*] prior to the engagement of the sub-processor, together with the information necessary to enable the controller to decide on the authorisation. It shall inform the data exporter of such engagement. The list of sub-processors already authorised by the controller can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*Specify time period*] in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

* 1. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. [[FN9](#bookmark=id.2gvnjns)] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
  2. The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
  3. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
  4. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

**CLAUSE 10**

**Data subject rights**

* 1. The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.
  2. The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
  3. In fulfilling its obligations under paragraphs ‎(a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

**CLAUSE 11**

**Redress**

* 1. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body[[FN11](#bookmark=id.w0xtvl)] at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph ‎(a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

* 1. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
  2. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
     1. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
     2. refer the dispute to the competent courts within the meaning of Clause 18.
  3. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
  4. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
  5. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

**CLAUSE 12**

**Liability**

* 1. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
  2. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
  3. Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
  4. The Parties agree that if the data exporter is held liable under paragraph ‎(c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
  5. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
  6. The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
  7. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

**CLAUSE 13**

**Supervision**

* 1. [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

* 1. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

**SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

**CLAUSE 14**

**Local laws and practices affecting compliance with the Clauses**

* 1. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
  2. The Parties declare that in providing the warranty in paragraph ‎(a), they have taken due account in particular of the following elements:
     1. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
     2. the laws and practices of the third country of destination – including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[[FN12](#bookmark=id.3g0lcje)];
     3. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
  3. The data importer warrants that, in carrying out the assessment under paragraph ‎(b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
  4. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
  5. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). The data exporter shall forward the notification to the controller.
  6. Following a notification pursuant to paragraph ‎(e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation, if appropriate in consultation with the controller. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the controller or the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

**CLAUSE 15**

**Obligations of the data importer in case of access by public authorities**

**15.1 Notification**

* 1. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
     1. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
     2. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

The data exporter shall forward the notification to the controller.

* 1. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
  2. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). The data exporter shall forward the information to the controller.
  3. The data importer agrees to preserve the information pursuant to paragraphs (a)‎ to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
  4. Paragraphs (a)‎ to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

**15.2 Review of legality and data minimisation**

* 1. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
  2. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. The data exporter shall make the assessment available to the controller.
  3. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

**SECTION IV – FINAL PROVISIONS**

**CLAUSE 16**

**Non-compliance with the Clauses and termination**

* 1. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
  2. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
  3. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
     1. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b)‎ and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
     2. the data importer is in substantial or persistent breach of these Clauses; or
     3. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority and the controller of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

* 1. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph ‎(c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
  2. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

**CLAUSE 17**

**Governing law**

[OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of \_\_\_\_\_\_\_ (*specify Member State*).]

[OPTION 2: These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of \_\_\_\_\_\_\_ (*specify Member State*).]

**CLAUSE 18**

**Choice of forum and jurisdiction**

* 1. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
  2. The Parties agree that those shall be the courts of \_\_\_\_\_ *(specify Member State)*.
  3. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
  4. The Parties agree to submit themselves to the jurisdiction of such courts.

**Official European Commission Footnotes**

[FN1](#bookmark=id.1l354xk): Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

[FN5](#bookmark=id.3vuw5zt): See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

[FN6](#bookmark=id.1ueyeci): The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

[FN9](#bookmark=id.1dtqche): This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[FN11](#bookmark=id.1dtqche): The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

[FN12](#bookmark=id.30mxrez): As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

**APPENDIX**

|  |
| --- |
| EXPLANATORY NOTE:  It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used. |

**ANNEX** **I**

**A. LIST OF PARTIES**

**Data exporter(s):** [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

1. Name: …………………….

Address: …………………….

Contact person's name, position and contact details: ……………...…

Activities relevant to the data transferred under these Clauses: …..…

Signature and date: ………………….…

Role (controller/processor): ……………………..…

2. …

**Data importer(s):** [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*]

1. Name: …………………….

Address: …………………….

Contact person's name, position and contact details: ……………...…

Activities relevant to the data transferred under these Clauses: …..…

Signature and date: ………………….…

Role (controller/processor): ……………………..…

2. …

**B. DESCRIPTION OF TRANSFER**

*Categories of data subjects whose personal data is transferred*

…………………….

*Categories of personal data transferred*

…………………….

*Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.*

…………………….

*The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).*

…………………….

*Nature of the processing*

…………………….

*Purpose(s) of the data transfer and further processing*

…………………….

*The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*

…………………….

*For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing*

…………………….

**C. COMPETENT SUPERVISORY AUTHORITY**

*Identify the competent supervisory authority/ies in accordance with Clause 13*

**ANNEX** **II**

**TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

|  |
| --- |
| EXPLANATORY NOTE:  The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers. |

*Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.*

*[Examples of possible measures:*

*Measures of pseudonymisation and encryption of personal data*

*Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services*

*Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident*

*Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing*

*Measures for user identification and authorisation*

*Measures for the protection of data during transmission*

*Measures for the protection of data during storage*

*Measures for ensuring physical security of locations at which personal data are processed*

*Measures for ensuring events logging*

*Measures for ensuring system configuration, including default configuration*

*Measures for internal IT and IT security governance and management*

*Measures for certification/assurance of processes and products*

*Measures for ensuring data minimisation*

*Measures for ensuring data quality*

*Measures for ensuring limited data retention*

*Measures for ensuring accountability*

*Measures for allowing data portability and ensuring erasure]*

*For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the* *controller and, for transfers from a processor to a sub-processor, to the data exporter*

**ANNEX** **III**

|  |
| --- |
| EXPLANATORY NOTE:  This Annex must be completed in case of the specific authorization of sub-processors (Clause 9(a), Option 1). |
|  |

The controller has authorised the use of the following sub-processors:

1. Name: ………………………

Address: ……………………

Contact person's name, position and contact details: …………………………..….

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): …………………………………..

2. ……..

Schedule 27

Intellectual Property Rights

# Schedule 27: Intellectual Property Rights

***[Guidance: Please review the guidance provided in Section 12 (Intellectual Property Rights) of the Front Sheet regarding which Option(s) are to be chosen for this Schedule Once the option has been selected in the Front Sheet please delete all unused options from this Schedule.]***

1. Intellectual Property Rights – General Provisions
   1. Except as expressly provided for in this Contract or otherwise agreed in writing:
      1. the Authority does not acquire any right, title or interest in or to the Intellectual Property Rights of the Supplier or its licensors, namely:
         1. the Supplier Software;
         2. the Third Party Software;
         3. the Third Party IPRs;
         4. the Supplier Background IPRs; and
         5. any Know-How, trade secrets or Confidential Information of the Supplier contained in any Specially Written Software or Project Specific IPR; and
      2. the Supplier does not acquire any right, title or interest in or to the Intellectual Property Rights of the Authority or its licensors, including:
2. the Authority Software;
   * + 1. the Government Data; and
       2. the Authority Background IPRs; and
     1. neither Party has the right to use the other Party’s IPRs, including any use of the other Party’s names, logos or trademarks.
   1. Where either Party acquires, by operation of law, ownership of Intellectual Property Rights that is inconsistent with the requirements of this Schedule 27 (*Intellectual Property Rights*), it must assign in writing the Intellectual Property Rights concerned to the other Party on the other Party’s request (whenever made).

[***Guidance: The cross references in Paragraph 1.3 are for Option 1 and should be updated for Option 2 to 2, 3 and 7; Option 3 to Paragraphs 2 and 5; and for Option 4 to 2 and 5.***]

* 1. If the Supplier becomes aware at any time, including after the Term, that, in respect of any Deliverable, the Authority has not received the licences to the Supplier Software, the Third Party Software, the Third Party IPRs and the Supplier Background IPRs required by Paragraphs 2, 3 and 5, the Supplier must, within 10 Working Days notify the Authority:
     1. the specific Intellectual Property Rights the Authority has not received licences to; and
     2. the Deliverables affected.
  2. Where a patent owned by the Supplier is infringed by the use of the Specially Written Software or Project Specific IPR by the Authority or any Replacement Supplier, the Supplier hereby grants to the Authority and the Replacement Supplier a non-exclusive, irrevocable, royalty-free, worldwide patent licence to use the infringing methods, materials or software.
  3. Unless otherwise agreed in writing, the Supplier will record in the table at Annex 1 to this Schedule and keep updated throughout the Term:
     1. any Specially Written Software and Project Specific IPR; and
     2. where:
        1. the Specially Written Software or Project Specific IPR adapts Supplier Software, Third Party Software, Third Party IPRs, or Supplier Background IPRs; or
        2. Supplier Software, Third Party Software, Third Party IPRs, or Supplier Background IPRs is embedded in, or forms an integral part of, the Specially Written Software or Project Specific IPR;

full details of the Supplier Software, Third Party Software, Third Party IPRs, or Supplier Background IPRs.

* 1. For the avoidance of doubt:
     1. except as provided for in Paragraph 2.2.3(c)(ii), the expiry or termination of this Contract does not of itself terminate the licences granted to the Authority under Paragraph 2;
     2. the award of this Contract or the ordering of any Deliverables does not constitute an authorisation by the Crown under:
        1. Sections 55 and 56 of the Patents Act 1977;
        2. section 12 of the Registered Designs Act 1949; or
        3. sections 240 to 243 of the Copyright, Designs and Patents Act 1988.

***[Guidance: For Option 1: Authority owns all Project Specific IPR and Specially Written Software, with limited Supplier rights to all Project Specific IPR and Specially Written Software in order to deliver the Contract, please include the following drafting.]***

## Option 1

1. Ownership and delivery of IPR created under the Contract
   1. Subject to Paragraph 1.1.1, the Supplier agrees to:
      1. transfer to the Authority, or procure the transfer to the Authority of all Intellectual Property Rights in the Specially Written Software and Project Specific IPRs, including:
         1. the Documentation, Source Code and the Object Code of the Specially Written Software; and
         2. all build instructions, test instructions, test scripts, test data, operating instructions and other documents and tools necessary for maintaining and supporting the Specially Written Software,

(together the **"Software Supporting Materials"**); and

* + 1. execute all such assignments required to transfer properly any rights in the Specially Written Software and Project Specific IPRs to the Authority.
  1. The Supplier must deliver to the Authority:
     1. the Specially Written Software;
     2. any software elements of the Project Specific IPR;
     3. relevant Documentation; and
     4. all related Software Supporting Materials,

within 5 Working Days of:

* + 1. either:
       1. initial release or deployment; or
       2. if a relevant Milestone has been identified in an Implementation Plan, Achievement of that Milestone; and
    2. each subsequent release or deployment of the Specially Written Software and any software elements of the Project Specific IPR.
  1. Where the Supplier delivers materials to the Authority under Paragraph 1.2, it must do so in a format specified by the Authority. Where the Authority specifies the material is to be delivered on media, the Authority becomes the owner of the media containing the material on delivery.

1. Use of Supplier or Third Party Non-COTS Software or Non-COTS Background IPR
   1. The Supplier must not use any:
      1. Supplier Non-COTS Software; or
      2. Supplier Non-COTS Background IPR;

in the provision of the Services or in any Deliverable (including in any Specially Written Software or in the software element of Project Specific IPRs) unless:

* + 1. in the case of Supplier Non-COTS Software and the software elements of Supplier Non-COTS Background IPR, it is:
       1. detailed in section 8 *(Software)* of the Front Sheet); or
       2. both:
          1. submitted to the Technical Board for review; and
          2. approved by the Authority; and
    2. in the case of non-software elements of Supplier Non-COTS Background IPR, it is approved by the Authority in writing.
  1. The Supplier must not use any:
     1. Third Party Non-COTS Software; or
     2. Third Party Non-COTS Background IPR,

in the provision of the Services or in any Deliverable (including in any Specially Written Software or in the software element of Project Specific IPRs) unless:

* + 1. in the case of Third Party Non-COTS Software and the software elements of Third Party Non-COTS Background IPR, it is:
       1. detailed in section 8 *(Software)* of the Front Sheet; or
       2. both:
          1. submitted to the Technical Board for review; and
          2. approved by the Authority; and
       3. one of the following conditions is met:
          1. the owner or an authorised licensor of the relevant IPR has granted the Authority a direct licence on the terms equivalent to those set out in Paragraph 5; or
          2. if the Supplier cannot, after commercially reasonable endeavours, meet the condition in Paragraph 2.2.3(c)(i), all the following conditions are met:

the Supplier has notified the Authority in writing giving details of:

what licence terms can be obtained from the relevant third party; and

whether there are providers which the Supplier could seek to use and the licence terms obtainable from those third parties;

the Authority approves the licence terms of one of those third parties; and

the owner and authorised licensor of the Third Party IPR has granted a direct licence of the Third Party IPR to the Authority on those terms; or

* + - * 1. if the Supplier cannot meet the conditions in Paragraphs 2.2.3(c)(i) and 2.2.3(c)(ii), the Authority has provided written approval to use the relevant IPR without a licence, with reference to the acts authorised and the specific IPR involved; or
    1. in the case of non-software elements of Third-Party Non-COTS Background IPR, it is approved by the Authority in writing.

1. Use of Supplier or Third Party COTS Software or COTS Background IPR
   1. The Supplier must not use any:
      1. Supplier COTS Software;
      2. Supplier COTS Background IPR;
      3. Third Party COTS Software; or
      4. Third Party COTS Background IPR,

in the provision of the Services (including in any Specially Written Software or in the software element of Project Specific IPRs) unless:

* + 1. in the case of Supplier COTS Software, Third Party COTS Software and the software elements of Supplier COTS Background IPR and Supplier COTS Background IPR, it is either:
       1. detailed in section 8 *(Software)* of the Front Sheet; or
       2. both:
          1. submitted to the Technical Board for review; and
          2. approved by the Authority; and
    2. all the following conditions are met:
       1. the Supplier has provided the Authority with the applicable terms for the IPRs (which must be at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available); and
       2. the Authority has not (in its absolute discretion) rejected those licence terms within 10 Working Days of the date on which they were provided to the Authority.

1. Licences granted by the Authority
   1. The Authority grants the Supplier a licence to the
      1. the Project-Specific IPR;
      2. the Specially Written Software;
      3. the Authority Software;
      4. the Government Data; and
      5. the Authority Background IPRs

that:

* + 1. is non-exclusive, royalty-free and non-transferable;
    2. is sub-licensable to any Sub-contractor where
       1. the Sub-contractor enters into a confidentiality undertaking with the Supplier on the same terms as set out in Annex 2 to this Schedule; and
       2. the sub-licence does not purport to provide the sub-licensee with any wider rights than those granted to the Supplier under this Paragraph;
    3. allows the Supplier and any sub-licensee to use, copy and adapt any licensed IPRs for the purpose of fulfilling its obligations under this Contract; and
    4. terminates at the later of:
       1. the expiry of the Term; or
       2. the end of any Termination Assistance Period.
  1. When the licence granted under Paragraph 4.1 terminates, the Supplier must, and must ensure that each Sub-contractor granted a sub-licence under Paragraph 4.1.7:
     1. immediately cease all use of the licensed IPR;
     2. either:
        1. at the discretion of the Authority, return or destroy documents and other tangible materials that contain any of the licensed IPR; or
        2. if the Authority has not made an election within six months of the termination of the licence, destroy the documents and other tangible materials that contain any of the licensed IPR; and
     3. ensure, so far as reasonably practicable, that any licensed IPR held in electronic, digital or other machine-readable form ceases to be readily accessible from any computer, word processor, voicemail system or any other device of the Supplier.

1. Licences in respect of Supplier Non-COTS Software and Supplier Non-COTS Background IPR
   1. Subject to the Authority approving the use of Supplier Non-COTS Software and Supplier Non-COTS Background IPR under Paragraph 2, the Supplier grants the Authority a Supplier Existing IPR Licence on the terms set out in Paragraph 5.3 in respect of each Deliverable where:
      1. the Supplier Non-COTS Software and Supplier Non-COTS Background IPR is embedded in the Deliverable;
      2. the Supplier Non-COTS Software and Supplier Non-COTS Background IPR is necessary for the Authority to use the Deliverable for any of the purposes set out in Paragraph 5.4; or
      3. the Deliverable is a customisation or adaptation of Supplier Non-COTS Software and Supplier Non-COTS Background IPR.
   2. The categories of Supplier Non-COTS Software and Supplier Non-COTS Background IPR set out in Paragraph 5.1 are mutually exclusive.
   3. The Supplier Existing IPR Licence granted by the Supplier to the Authority is a non-exclusive, perpetual, royalty-free, irrevocable, transferable, sub-licensable, worldwide licence that:
      1. in the case of Supplier Non-COTS Software and Supplier Non-COTS Background IPR embedded in a Deliverable:
         1. has no restriction on the identity of any transferee or sub-licensee;
         2. is sub-licensable for any of the purposes set out in Paragraph 5.4;
         3. allows the Authority and any transferee or sub-licensee to use, copy and adapt the Supplier Non-COTS Software and Supplier Non-COTS Background IPR for any of the purposes set out in Paragraph 5.4; and
      2. in the case of Supplier Non-COTS Software and Supplier Non-COTS Background IPR that is necessary for the Authority to use the Deliverable for its intended purpose or has been customised or adapted to provide the Deliverable:
         1. allows the Authority and any transferee or sublicensee to use and copy, but not adapt, disassemble or reverse engineer the relevant Supplier Non-COTS Software and Supplier Non-COTS Background IPR for any of the purposes set out in Paragraph 5.4;
         2. is transferrable to only:
            1. a Crown Body;
            2. any body (including any private sector body) that performs or carries out any of the functions or activities that the Authority had previously performed or carried out; or
            3. a person or organisation that is not a direct competitor of the Supplier; where that transferee:

enters into a direct arrangement with the Supplier in the form set out in section 8 *(Software)* of the Front Sheet; or

enters into a confidentiality arrangement with the Authority in terms equivalent to those set out in set out in Clause 19 (*Confidentiality*);

* + - 1. is sub-licensable to the Replacement Supplier (including where the Replacement Supplier is a competitor of the Supplier) where the Replacement Supplier:
         1. enters into a direct arrangement with the Supplier in the form set out in section 8 *(Software)* of the Front Sheet; or
         2. enters into a confidentiality arrangement with the Authority in terms equivalent to those set out in set out in Clause 19 (*Confidentiality*);
    1. includes a perpetual, royalty-free, non-exclusive licence to use, copy and adapt any Know-How, trade secrets or Confidential Information of the Supplier contained within any Supplier Non-COTS Software and Supplier Non-COTS Background IPR;
    2. continues in effect following the expiry or earlier termination of this Contract; and
    3. is subject to the restrictions that:
       1. no sub-licence granted to the Supplier Non-COTS Software and Supplier Non-COTS Background IPR shall purport to provide the sub-licensee with any wider rights than those granted to the Authority under this Paragraph; and
       2. any transferee or sublicensee of the Supplier Non-COTS Software and Supplier Non-COTS Background IPR must either:
          1. enter into a direct arrangement with the Supplier in the form set out in section 8 *(Software)* of the Front Sheet); or
          2. enter into a confidentiality arrangement with the Authority in terms equivalent to those set out in set out in Clause 19 (*Confidentiality*).
  1. For the purposes of Paragraphs 5.1 and 5.3, the relevant purposes are:
     1. to allow the Authority or any End User to receive and use the Deliverables;
     2. to commercially exploit (including by publication under Open Licence) the Project Specific IPR, Specially Written Software and Software Supporting Materials; and
     3. for any purpose relating to the exercise of the Authority’s (or, if the Authority is a Public Sector Body, any other Public Sector Body’s) business or function.
  2. Where the legal status of the Authority changes, such that it ceases to be a Crown Body:
     1. the Supplier Existing IPR Licence is unaffected; and
     2. any successor body of the Authority that is a Crown Body shall have the benefit of the Supplier Existing IPR Licence.
  3. Where the Supplier Existing IPR Licence is transferred under Paragraph 5.3.1(a) or 5.3.2(b) or there is a change in the Authority’s legal status to which Paragraph 5.5 applies, the transferee or successor body do not acquire any wider rights than those granted to the Authority under this Paragraph.

1. Open Licence Publication
   1. Subject to Paragraph 6.8, the Supplier agrees that the Authority may at its sole discretion publish under Open Licence all or part of the Project Specific IPR, the Specially Written Software or the Software Supporting Materials.
   2. The Supplier warrants that:
      1. the Project Specific IPR, the Specially Written Software or the Software Supporting Materials are suitable for release under Open Licence;
      2. in developing Project Specific IPR, the Specially Written Software or the Software Supporting Materials it has used reasonable endeavours to ensure that:
         1. the publication by the Authority will not:
            1. allow a third party to use them in to compromise the operation, running or security of the Specially Written Software, the Project Specific IPRs, the Authority System or the Supplier System;
            2. cause any harm or damage to any party using them; or
            3. breach the rights of any third party; and
         2. they do not contain any material which would bring the Authority into disrepute if published.
   3. The Supplier must not include in the Project Specific IPR, the Specially Written Software or the Software Supporting Materials provided for publication by Open Licence any Supplier Software, Supplier Background IPR, or Know-How, trade secrets or Confidential Information of the Supplier contained in any Specially Written Software or Project Specific IPR unless the Supplier consents to:
      1. their publication by the Authority under Open Licence; and
      2. their subsequent licence and treatment as Open Licence under the terms of the licence chosen by the Authority.
   4. The Authority will not be liable in the event that any Supplier Software, Supplier Background IPR, or Know-How, trade secrets or Confidential Information of the Supplier contained in any Specially Written Software or Project Specific IPR is included in the Open Licence Publication Material published by the Authority
   5. The Supplier must supply any or all the Project Specific IPR, the Specially Written Software or the Software Supporting Materials in a format (whether it is provided in any other format or not) suitable for publication under an Open Licence (the **"Open Licence Publication Material"**) within 30 Working Days of written request from the Authority (**"Authority Open Licence Request"**).
   6. The Supplier may within 15 Working Days of Authority Open Licence Request under Paragraph 6.5 request in writing that the Authority excludes all or part of:
      1. the Project Specific IPR, the Specially Written Software or the Software Supporting Materials Items; or
      2. the Supplier Software, the Third Party Software, the Third Party IPRs, the Supplier Background IPRs, or any Know-How, trade secrets or Confidential Information of the Supplier contained in any Specially Written Software or Project Specific IPR that would otherwise be included in the Open Licence Publication Material supplied to the Authority pursuant to Paragraph 6.5,

from Open Licence publication.

* 1. The Supplier’s request under Paragraph 6.5 must include the Supplier’s assessment of the impact the Authority’s agreeing to the request would have on its ability to publish other Project Specific IPR, Specially Written Software or Software Supporting Materials under an Open Licence.
  2. Any decision to Approve any such request from the Supplier under Paragraph 6.5 shall be at the Authority’s sole discretion, not to be unreasonably withheld or delayed, or made subject to unreasonable conditions.

***[Guidance: For Option 2: Authority owns all Project Specific IPR and Specially Written Software with non-exclusive Supplier rights, please include the following drafting:]***

## Option 2

1. Ownership and delivery of IPR created under the Contract
   1. Subject to Paragraph 1.1.1, the Supplier agrees to
      1. transfer to the Authority, or procure the transfer to the Authority of all Intellectual Property Rights in the Specially Written Software and Project Specific IPRs, including:
         1. the Documentation, Source Code and the Object Code of the Specially Written Software; and
         2. all build instructions, test instructions, test scripts, test data, operating instructions and other documents and tools necessary for maintaining and supporting the Specially Written Software,

(together the **"Software Supporting Materials"**); and

* + 1. execute all such assignments required to transfer properly any rights in the Specially Written Software and Project Specific IPRs to the Authority.
  1. The Supplier must deliver to the Authority:
     1. the Specially Written Software;
     2. any software elements of the Project Specific IPR;
     3. relevant Documentation; and
     4. all related Software Supporting Materials,

within seven days of:

* + 1. either:
       1. initial release or deployment; or
       2. if a relevant Milestone has been identified in an Implementation Plan, Achievement of that Milestone; and
    2. each subsequent release or deployment of the Specially Written Software and any software elements of the Project Specific IPR.
  1. Where the Supplier delivers materials to the Authority under Paragraph 1.2, it must do so in a format specified by the Authority. Where the Authority specifies the material is to be delivered on media, the Authority becomes the owner of the media containing the material on delivery.

1. Use of Supplier or Third Party Non-COTS Software or Non-COTS Background IPR
   1. The Supplier must not use any:
      1. Supplier Non-COTS Software; or
      2. any Supplier Non-COTS Background IPR;

in the provision of the Services or any Deliverables (including in any Specially Written Software or in the software element of Project Specific IPRs) unless:

* + 1. in the case of Supplier Non-COTS Software and the software elements of Supplier Non-COTS Background IPR, it is either:
       1. detailed in section 8 *(Software)* of the Front Sheet; or
       2. both:
          1. submitted to the Technical Board for review; and
          2. approved by the Authority; or
    2. in the case of non-software elements of Supplier Non-COTS Background IPR, it is approved by the Authority in writing.
  1. The Supplier must not use any:
     1. Third Party Non-COTS Software; or
     2. Third Party Non-COTS Background IPR,

in the provision of the Services or in any Deliverable (including in any Specially Written Software or in the software element of Project Specific IPRs) unless:

* + 1. in the case of Third Party Non-COTS Software and the software elements of Third Party Non-COTS Background IPR, it is either:
       1. detailed in section 8 *(Software)* of the Front Sheet; or
       2. both:
          1. submitted to the Technical Board for review; and
          2. approved by the Authority; and
       3. one of the following conditions is met:
          1. the owner or an authorised licensor of the relevant IPR has granted the Authority a direct licence on the terms equivalent to those set out in Paragraph 7; or
          2. if the Supplier cannot, after commercially reasonable endeavours, meet the condition in Paragraph 2.2.3(c)(i), all the following conditions are met:

the Supplier has notified the Authority in writing giving details of:

what licence terms can be obtained from the relevant third party; and

whether there are providers which the Supplier could seek to use and the licence terms obtainable from those third parties;

the Authority approves the licence terms of one of those third parties; and

the owner and authorised licensor of the Third Party IPR has granted a direct licence of the Third Party IPR to the Authority on those terms; or

* + - * 1. if the Supplier cannot meet the conditions in Paragraphs 2.2.3(c)(i) and 2.2.3(c)(ii), the Authority has provided written approval to use the relevant IPR without a licence, with reference to the acts authorised and the specific IPR involved; or
    1. in the case of non-software elements of Third-Party Non-COTS Background IPR, it is approved by the Authority in writing.

1. Use of Supplier or Third Party COTS Software or COTS Background IPR
   1. The Supplier must not use any:
      1. Supplier COTS Software;
      2. Supplier COTS Background IPR;
      3. Third Party COTS Software; or
      4. Third Party COTS Background IPR,

in the provision of the Services (including in any Specially Written Software or in the software element of Project Specific IPRs) unless:

* + 1. in the case of Supplier COTS Software, Third Party COTS Software and the software elements of Supplier COTS Background IPR and Supplier COTS Background IPR, it is either:
       1. detailed in section 8 *(Software)* of the Front Sheet; or
       2. both:
          1. submitted to the Technical Board for review; and
          2. approved by the Authority; and
    2. all the following conditions are met:
       1. the Supplier has provided the Authority with the applicable terms for the IPRs (which must be at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available); and
       2. the Authority has not (in its absolute discretion) rejected those licence terms within 10 Working Days of the date on which they were provided to the Authority.

1. Licences granted by the Authority
   1. Subject to Paragraph 5, the Authority grants the Supplier a licence to the
      1. the Project-Specific IPR;
      2. the Specially Written Software;
      3. the Authority Software;
      4. the Government Data; and
      5. the Authority Background IPRs;

that:

* + 1. is non-exclusive, royalty-free and non-transferable;
    2. is sub-licensable to any Sub-contractor where;
       1. the Sub-contractor enters into a confidentiality undertaking with the Supplier on the same terms as set out in Annex 2 to this Schedule; and
       2. the sub-licence does not purport to provide the sub-licensee with any wider rights than those granted to the Supplier under this Paragraph;
    3. allows the Supplier and any sub-licensee to use, copy and adapt any licensed IPRs for the purpose of:
       1. fulfilling its obligations under this Contract; and
       2. commercially exploiting the Project Specific IPR and Specially Written Software; and
    4. continues in effect following the expiry or earlier termination of this Contract.
  1. When the licence granted under Paragraph 4.1:
     1. terminates in accordance with Paragraph 5; or
     2. no longer has effect at the end of the Term or the expiry of any Termination Assistance Period (whichever is the later),

the Supplier must, and must ensure that each Sub-contractor granted a sub-licence under Paragraph 4.1.7:

* + 1. immediately cease all use of the licensed IPR;
    2. either:
       1. at the discretion of the Authority, return or destroy documents and other tangible materials that contain any of the licensed IPR; or
       2. if the Authority has not made an election within six months of the termination of the licence, destroy the documents and other tangible materials that contain any of the licensed IPR; and
    3. ensure, so far as reasonably practicable, that any licensed IPR held in electronic, digital or other machine-readable form ceases to be readily accessible from any computer, word processor, voicemail system or any other device of the Supplier.

1. Authority approval for Supplier to exploit IPR created under Contract
   1. Before using, copying or adapting any:
      1. Project-Specific IPR;
      2. Specially Written Software;
      3. Authority Software;
      4. Government Data; and
      5. Authority Background IPRs;

for any purpose other than fulfilling its obligations under this Contract, the Supplier must seek the approval of the Authority in accordance with the provisions of this Paragraph.

* 1. The Authority may terminate any licence it grants under this Paragraph by notice in writing with immediate effect where the Supplier breaches any condition in that licence.

***[Guidance: Where Option 5 is used, replace Paragraphs 5.3, 5.4 and 5.5 with the Paragraphs in Option 5.]***

* 1. The Supplier must provide a proposal setting out:
     1. the purpose for which it proposes to use the IPR;
     2. the activities the Supplier proposes to undertake with or in respect of the IPR;
     3. such further information as the Authority may reasonably require to properly consider the proposal.
  2. The Authority may only refuse the Supplier’s proposal where it considers that if the Supplier were to implement the proposal it would harm:
     1. the Authority’s reputation; or
     2. the Authority’s interests.
  3. Where the Authority has not:
     1. approved or declined the proposal; or
     2. required further information,

within 20 Working Days of the later of:

* + 1. the date the proposal was first provided to the Authority; or
    2. the date on which further information was provided to the Authority,

then the proposal is, for the purposes of this Contract, approved.

1. Provision of information on Project Specific IPR and Specially Written Software
   1. The Authority may, at any time, require the Supplier to provide information on:
      1. the purposes, other than for the purposes of this Contract, for which the Supplier uses Project Specific IPR and Specially Written Software; and
      2. the activities the Supplier undertakes, other than under this Contract, with or in respect of the Project Specific IPR and Specially Written Software.
   2. The Supplier must provide the information required by the Authority:
      1. within 20 Working Days of the date of the requirement; and
      2. in the form and with the content specified by the Authority.
2. Licences in respect of Supplier Non-COTS Software and Supplier Non-COTS Background IPR
   1. Subject to the Authority approving the use of Supplier Non-COTS Software and Supplier Non-COTS Background IPR under Paragraph 2, the Supplier grants the Authority a Supplier Existing IPR Licence on the terms set out in Paragraph 7.3 in respect of each Deliverable where:
      1. the Supplier Non-COTS Software and Supplier Non-COTS Background IPR is embedded in the Deliverable;
      2. the Supplier Non-COTS Software and Supplier Non-COTS Background IPR is necessary for the Authority to use the Deliverable for any of the purposes set out in Paragraph 7.4; or
      3. the Deliverable is a customisation or adaptation of Supplier Non-COTS Software and Supplier Non-COTS Background IPR.
   2. The categories of Supplier Non-COTS Software and Supplier Non-COTS Background IPR set out in Paragraph 7.1 are mutually exclusive.
   3. The Supplier Existing IPR Licence granted by the Supplier to the Authority is a non-exclusive, perpetual, royalty-free, irrevocable, transferable, sub-licensable, worldwide licence that:
      1. in the case of Supplier Non-COTS Software and Supplier Non-COTS Background IPR embedded in a Deliverable:
         1. has no restriction on the identity of any transferee or sub-licensee;
         2. is sub-licensable for any of the purposes set out in Paragraph 7.4;
         3. allows the Authority and any transferee or sub-licensee to use, copy and adapt the Supplier Non-COTS Software and Supplier Non-COTS Background IPR for any of the purposes set out in Paragraph 7.4; and
      2. in the case of Supplier Non-COTS Software and Supplier Non-COTS Background IPR that is necessary for the Authority to use the Deliverable for its intended purpose or has been customised or adapted to provide the Deliverable:
         1. allows the Authority and any transferee or sublicensee to use and copy, but not adapt, disassemble or reverse engineer the relevant Supplier Non-COTS Software and Supplier Non-COTS Background IPR for any of the purposes set out in Paragraph 7.4;
         2. is transferrable to only:
            1. a Crown Body;
            2. any body (including any private sector body) that performs or carries out any of the functions or activities that the Authority had previously performed or carried out; or
            3. a person or organisation that is not a direct competitor of the Supplier; where that transferee:

enters into a direct arrangement with the Supplier in the form set out in Annex 2 to this Schedule; or

enters into a confidentiality arrangement with the Authority in terms equivalent to those set out in set out in Clause 19 (*Confidentiality*);

* + - 1. is sub-licensable to the Replacement Supplier (including where the Replacement Supplier is a competitor of the Supplier) where the Replacement Supplier:
         1. enters into a direct arrangement with the Supplier in the form set out in Annex 2 to this Schedule; or
         2. enters into a confidentiality arrangement with the Authority in terms equivalent to those set out in set out in Clause 19 (*Confidentiality*);
    1. includes a perpetual, royalty-free, non-exclusive licence to use, copy and adapt any Know-How, trade secrets or Confidential Information of the Supplier contained within any Supplier Non-COTS Software and Supplier Non-COTS Background IPR;
    2. continues in effect following the expiry or earlier termination of this Contract; and
    3. is subject to the restrictions that:
       1. no sub-licence granted to the Supplier Non-COTS Software and Supplier Non-COTS Background IPR shall purport to provide the sub-licensee with any wider rights than those granted to the Authority under this Paragraph;
       2. any transferee or sublicensee of the Supplier Non-COTS Software and Supplier Non-COTS Background IPR must either:
          1. enter into a direct arrangement with the Supplier in the form set out in Annex 2 of this Schedule; or
          2. enter into a confidentiality arrangement with the Authority in terms equivalent to those set out in set out in Clause 19 (*Confidentiality*).
  1. For the purposes of Paragraphs 7.1 and 7.3, the relevant purposes are:
     1. to allow the Authority or any End User to receive and use the Deliverables;
     2. to commercially exploit the Project Specific IPR, Specially Written Software and Software Supporting Materials; and
     3. for any purpose relating to the exercise of the Authority’s (or, if the Authority is a Public Sector Body, any other Public Sector Body’s) business or function.
  2. Where the legal status of the Authority changes, such that it ceases to be a Crown Body:
     1. the Supplier Existing IPR Licence is unaffected; and
     2. any successor body of the Authority that is a Crown Body shall have the benefit of the Supplier Existing IPR Licence.
  3. Where the Supplier Existing IPR Licence is transferred under Paragraph 7.3.1(a) or 7.3.2(b) or there is a change in the Authority’s legal status to which Paragraph 7.5 applies, the transferee or successor body do not acquire any wider rights than those granted to the Authority under this Paragraph.

***[Guidance: For Option 3: Supplier ownership of all Project Specific IPR and Specially Written Software with Authority rights for the current contract only, please include the following drafting.]***

## Option 3

1. Ownership of IPR created under the Contract
   1. Subject to Paragraph 1.1.1, the Authority agrees to
      1. transfer to the Supplier, or procure the transfer to the Supplier, of all Intellectual Property Rights in the Specially Written Software and Project Specific IPRs not already vesting in the Supplier, including:
         1. the Documentation, Source Code and the Object Code of the Specially Written Software; and
         2. all build instructions, test instructions, test scripts, test data, operating instructions and other documents and tools necessary for maintaining and supporting the Specially Written Software,

(together the **"Software Supporting Materials"**); and

* + 1. execute all such assignments required to transfer properly any rights in the Specially Written Software and Project Specific IPRs to the Supplier.
  1. If, within three years of its creation, the Supplier:
     1. is not commercially exploiting any Specially Written Software, Project Specific IPRs or Software Supporting Materials; or
     2. where the Supplier is not commercially exploiting that IPR, is not, to the satisfaction of the Authority, using its best endeavours to do so,

then, on written request from the Authority:

* + 1. the Supplier must promptly assign to the Authority the Specially Written Software, Project Specific IPRs and Software Supporting Materials, or any specified items of that IPR; and
    2. the licence to the Authority Software, Government Data and Authority Background IPRs granted under Paragraph 6.1 (insofar as it relates to the commercial exploitation of the Project Specific IPR, the Specially Written Software or the Software Supporting Materials) terminates either:
       1. on the date specified in the notice; or
       2. where no date is specified in the notice, on the date the notice is received by the Supplier.
  1. Each Party shall bear its own costs of preparing and executing any assignment required by this Paragraph.

1. Licence of Supplier IPR
   1. The Supplier grants the Authority a licence on the terms set out in Paragraph 2.3 in respect of each Deliverable where Specially Written Software, Project Specific IPRs, Software Supporting Materials, Supplier Software or Supplier Background IPRs are:
      1. is embedded in the Deliverable;
      2. is necessary for the Authority to use the Deliverable; or
      3. has been customised or adapted to create the Deliverable.
   2. The categories of relevant IPR set out in Paragraph 2.1 are mutually exclusive.
   3. The licence referred to in Paragraph 2.1 is a non-exclusive, royalty-free, irrevocable, transferable, sub-licensable, worldwide licence that:
      1. in the case of relevant IPR embedded in a Deliverable or is used to provide the Deliverable:
         1. is sub-licensable;
         2. has no restriction on the identity of any transferee or sub-licensee;
         3. allows the Authority and any transferee or sub-licensee to use, copy and adapt the relevant IPR for any of the purposes set out in Paragraph 2.4;
      2. in the case of relevant IPR that is necessary for the Authority to receive or use the Deliverable:
         1. allows the Authority and any transferee or sublicensee to use and copy, but not adapt, disassemble or reverse engineer the relevant IPR for any of the purposes set out in Paragraph 2.4;
         2. is transferrable to only:
            1. a Crown Body;
            2. any body (including any private sector body) that performs or carries out any of the functions or activities that the Authority had previously performed or carried out; or
            3. a person or organisation that is not a direct competitor of the Supplier, where that transferee:

enters into a direct arrangement with the Supplier in the form set out in Annex 2 of this Schedule; or

enters into a confidentiality arrangement with the Authority in terms equivalent to those set out in set out in Clause 19 (*Confidentiality*);

* + - 1. is sub-licensable to the Replacement Supplier (including where the Replacement Supplier is a competitor of the Supplier) where the Replacement Supplier:
         1. enters into a direct arrangement with the Supplier in the form set out in Annex 2 of this Schedule; or
         2. enters into a confidentiality arrangement with the Authority in terms equivalent to those set out in set out in Clause 19 (*Confidentiality*);
    1. expires at the later of
       1. the expiry of the Term; or
       2. the expiry of any Termination Assistance Period; and
    2. is subject to the restrictions that
       1. each transferee or sub-licensee either:
          1. enters into a direct arrangement with the Supplier in the form set out in Annex 2 to this Schedule; or
          2. enters into a confidentiality arrangement with the Authority in terms equivalent to those set out in set out in Clause 19 (*Confidentiality*); and
       2. no sub-licence granted to the relevant IPR shall purport to provide the sub-licensee with any wider rights than those granted to the Authority under this Paragraph.
  1. For the purposes of Paragraphs 2.1 and 2.3, the relevant purposes are:
     1. to allow the Authority or any End User to receive and use the Deliverables; and
     2. for any purpose relating to the exercise of the Authority’s (or, if the Authority is a Public Sector Body, any other Public Sector Body’s) business or function.
  2. Where the legal status of the Authority changes, such that it ceases to be a Crown Body:
     1. the licence granted under Paragraph 2.3 is unaffected; and
     2. any successor body of the Authority that is a Crown Body shall have the benefit of the licence granted under Paragraph 2.3.
  3. Where the licence granted under Paragraph 2.3 is transferred under Paragraph 2.3.1(b) or 2.3.2(b) or there is a change in the Authority’s legal status to which Paragraph 2.5 applies, the transferee or successor body do not acquire any wider rights than those granted to the Authority under this Paragraph.

1. Authority approval for Supplier to exploit Authority IPR
   1. Before using, copying or adapting any:
      1. Authority Software;
      2. Government Data; and
      3. Authority Background IPRs;

for any purpose other than fulfilling its obligations under this Contract, the Supplier must seek the approval of the Authority in accordance with the provisions of this Paragraph.

* 1. The Authority may terminate any licence it grants under this Paragraph by notice in writing with immediate effect where the Supplier breaches any condition in that licence.

***[Guidance: Where Option 5 is used, replace Paragraphs 3.3, 3.4 and 3.5 with the Paragraphs in Option 5.]***

* 1. The Supplier must provide a proposal setting out:
     1. the purpose for which it proposes to use the IPR;
     2. the activities the Supplier proposes to undertake with or in respect of the IPR;
     3. such further information as the Authority may reasonably require to properly consider the proposal.
  2. The Authority may only refuse the Supplier’s proposal where it considers that if the Supplier were to implement the proposal it would harm:
     1. the Authority’s reputation; or
     2. the Authority’s interests.
  3. Where the Authority has not:
     1. approved or declined the proposal; or
     2. required further information,

within 20 Working Days of the later of:

* + 1. the date the proposal was first provided to the Authority; or
    2. the date on which further information was provided to the Authority,

then the proposal is, for the purposes of this Contract, approved.

1. Provision of information on Project Specific IPR and Specially Written Software
   1. The Authority may, at any time, require the Supplier to provide information on:
      1. the purposes, other than for the purposes of this Contract, for which the Supplier uses Project Specific IPR and Specially Written Software; and
      2. the activities the Supplier undertakes, other than under this Contract, with or in respect of the Project Specific IPR and Specially Written Software.
   2. The Supplier must provide the information required by the Authority:
      1. within 20 Working Days of the date of the requirement; and
      2. in the form and with the content specified by the Authority.
2. Use of Third Party IPR
   1. The Supplier must not use any:
      1. Third Party Non-COTS Software; or
      2. Third Party Non-COTS Background IPR,

in the provision of the Services (including in any Specially Written Software or in the software element of Project Specific IPRs) unless one of the following conditions is met:

* + 1. the owner or an authorised licensor of the relevant IPR has granted the Authority a direct licence on the terms equivalent to those set out in Paragraph 2; or
    2. if the Supplier cannot, after commercially reasonable endeavours, meet the condition in Paragraph 5.1.3, all the following conditions are met:
       1. the Supplier has notified the Authority in writing giving details of:
          1. what licence terms can be obtained from the relevant third party; and
          2. whether there are providers which the Supplier could seek to use and the licence terms obtainable from those third parties;
       2. the Authority approves the licence terms of one of those third parties; and
       3. the owner and authorised licensor of the Third Party IPR has granted a direct licence of the Third Party IPR to the Authority on those terms; or
    3. if the Supplier cannot meet the conditions in Paragraphs 5.1.3 and 5.1.4, the Authority has provided written approval to use the relevant IPR without a licence, with reference to the acts authorised and the specific IPR involved.
  1. The Supplier must not use any:
     1. Third Party COTS Software; or
     2. Third Party COTS Background IPR,

in the provision of the Services (including in any Specially Written Software or in the software element of Project Specific IPRs) unless the following conditions are met:

* + 1. the Supplier has provided the Authority with the applicable terms for the IPRs (which must be at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available); and
    2. the Authority has not (in its absolute discretion) rejected those licence terms within 10 Working Days of the date on which they were provided to the Authority.

1. Licences granted by the Authority
   1. Subject to Paragraph 3, the Authority grants the Supplier a licence to the
      1. the Authority Software;
      2. the Government Data; and
      3. the Authority Background IPRs

that:

* + 1. is perpetual, non-exclusive, royalty-free and non-transferable;
    2. is sub-licensable to any Sub-contractor where:
       1. the Sub-contractor enters into a confidentiality undertaking with the Supplier on the same terms as set out in Annex 2 to this Schedule; and
       2. the sub-licence does not purport to provide the sub-licensee with any wider rights than those granted to the Supplier under this Paragraph;
    3. allows the Supplier and any sub-licensee to use, copy and adapt any licensed IPRs for the purpose of:
       1. fulfilling its obligations under this Contract; or
       2. commercially exploiting the Project Specific IPR, the Specially Written Software or the Software Supporting Materials.
  1. When the licence granted under Paragraph 6.1:
     1. terminates in accordance with Paragraph 3; or
     2. no longer has effect at the end of the Term or the expiry of any Termination Assistance Period (whichever is the later),

the Supplier must, and must ensure that each Sub-contractor granted a sub-licence under Paragraph 6.1.5:

* + 1. immediately cease all use of the licensed IPR;
    2. either:
       1. at the discretion of the Authority, return or destroy documents and other tangible materials that contain any of the licensed IPR; or
       2. if the Authority has not made an election within six months of the termination of the licence, destroy the documents and other tangible materials that contain any of the licensed IPR; and
    3. ensure, so far as reasonably practicable, that any licensed IPR held in electronic, digital or other machine-readable form ceases to be readily accessible from any computer, word processor, voicemail system or any other device of the Supplier.

***[Guidance: For Option 4: Supplier ownership of all Specially Written Software and Project Specific IPR with Authority rights for the current contract and broader public sector functions, please include the following drafting.]***

## Option 4

1. Ownership of IPR created under the Contract
   1. Subject to Paragraph 1.1.1, the Authority agrees to
      1. transfer to the Supplier, or procure the transfer to the Supplier, of all Intellectual Property Rights in the Specially Written Software and Project Specific IPRs not already vesting in the Supplier, including:
         1. the Documentation, Source Code and the Object Code of the Specially Written Software; and
         2. all build instructions, test instructions, test scripts, test data, operating instructions and other documents and tools necessary for maintaining and supporting the Specially Written Software,

(together the **"Software Supporting Materials"**); and

* + 1. execute all such assignments required to transfer properly any rights in the Specially Written Software and Project Specific IPRs to the Supplier.
  1. If, within three years of its creation, the Supplier:
     1. is not commercially exploiting any Specially Written Software, Project Specific IPRs or Software Supporting Materials; or
     2. where the Supplier is not commercially exploiting that IPR, is not, to the satisfaction of the Authority, using its best endeavours to do so,

then, on written request from the Authority:

* + 1. the Supplier must promptly assign to the Authority the Specially Written Software, Project Specific IPRs and Software Supporting Materials, or any specified items of that IPR; and
    2. the licence to the Authority Software, Government Data and Authority Background IPRs granted under Paragraph 6.1 (insofar as it relates to the commercial exploitation of the Project Specific IPR, the Specially Written Software or the Software Supporting Materials) terminates either:
       1. on the date specified in the notice; or
       2. where no date is specified in the notice, on the date the notice is received by the Supplier.
  1. Each Party shall bear its own costs of preparing and executing any assignment required by this Paragraph.

1. Licence of Supplier IPR
   1. The Supplier grants the Authority a licence on the terms set out in Paragraph 2.3 in respect of each Deliverable where Specially Written Software, Project Specific IPRs, Software Supporting Materials, Supplier Software or Supplier Background IPRs are:
      1. is embedded in the Deliverable;
      2. is necessary for the Authority to use the Deliverable;
      3. in the case of Specially Written Software, Project Specific IPRs, Software Supporting Materials is used to provide the Deliverable;
      4. in the case of Supplier Software or Supplier Background IPRs has been customised or adapted to create the Deliverable.
   2. The categories of relevant IPR set out in Paragraph 2.1 are mutually exclusive.
   3. The licence referred to in Paragraph 2.1 is a perpetual, non-exclusive, royalty-free, irrevocable, transferable, sub-licensable, worldwide licence that:
      1. in the case of relevant IPR embedded in a Deliverable, is used to provide the Deliverable, or where the relevant IPR has been customised or adapted to create the Deliverable:
         1. is sub-licensable;
         2. has no restriction on the identity of any transferee or sub-licensee;
         3. allows the Authority and any transferee or sub-licensee to use, copy and adapt the relevant IPR for any of the purposes set out in Paragraph 2.4;
      2. in the case of relevant IPR that is necessary for the Authority to receive or use the Deliverable:
         1. allows the Authority and any transferee or sublicensee to use and copy, but not adapt, disassemble or reverse engineer the relevant IPR for any of the purposes set out in Paragraph 2.4;
         2. is transferrable to only:
            1. a Crown Body;
            2. any body (including any private sector body) that performs or carries out any of the functions or activities that the Authority had previously performed or carried out; or
            3. a person or organisation that is not a direct competitor of the Supplier, where that transferee:

enters into a direct arrangement with the Supplier in the form set out in Annex 2 of this Schedule; or

enters into a confidentiality arrangement with the Authority in terms equivalent to those set out in set out in Clause 19 (*Confidentiality*);

* + - 1. is sub-licensable to the Replacement Supplier (including where the Replacement Supplier is a competitor of the Supplier) where the Replacement Supplier:
         1. enters into a direct arrangement with the Supplier in the form set out in Annex 2 to this Schedule; or
         2. enters into a confidentiality arrangement with the Authority in terms equivalent to those set out in set out in Clause 19 (*Confidentiality*);
    1. expires at the later of
       1. the expiry of the Term; or
       2. the expiry of any Termination Assistance Period; and
    2. is subject to the restrictions that
       1. each transferee or sub-licensee either:
          1. enters into a direct arrangement with the Supplier in the form set out in Annex 2 to this Schedule; or
          2. enters into a confidentiality arrangement with the Authority in terms equivalent to those set out in set out in Clause 19 (*Confidentiality*) ; and
       2. no sub-licence granted to the relevant IPR shall purport to provide the sub-licensee with any wider rights than those granted to the Authority under this Paragraph.
  1. For the purposes of Paragraphs 2.1 and 2.3, the relevant purposes are:
     1. to allow the Authority or any End User to receive and use the Deliverables; and
     2. for any purpose relating to the exercise of the Authority’s (or, if the Authority is a Public Sector Body, any other Public Sector Body’s) business or function.
  2. Where the legal status of the Authority changes, such that it ceases to be a Crown Body:
     1. the licence granted under Paragraph 2.3 is unaffected; and
     2. any successor body of the Authority that is a Crown Body shall have the benefit of the licence granted under Paragraph 2.3.
  3. Where the licence granted under Paragraph 2.3 is transferred under Paragraph 2.3.1(b) or 2.3.2(b) or there is a change in the Authority’s legal status to which Paragraph 2.5 applies, the transferee or successor body do not acquire any wider rights than those granted to the Authority under this Paragraph.

1. Authority approval for Supplier to exploit Authority IPR
   1. Before using, copying or adapting any:
      1. Authority Software;
      2. Government Data; and
      3. Authority Background IPRs;

for any purpose other than fulfilling its obligations under this Contract, the Supplier must seek the approval of the Authority in accordance with the provisions of this Paragraph.

* 1. The Authority may terminate any licence it grants under this Paragraph by notice in writing with immediate effect where the Supplier breaches any condition in that licence.

***[Guidance: Where Option 5 is used, replace Paragraphs 3.3, 3.4, 3.5 with the Paragraphs in Option 5.]***

* 1. The Supplier must provide a proposal setting out:
     1. the purpose for which it proposes to use the IPR;
     2. the activities the Supplier proposes to undertake with or in respect of the IPR;
     3. such further information as the Authority may reasonably require to properly consider the proposal.
  2. The Authority may only refuse the Supplier’s proposal where it considers that if the Supplier were to implement the proposal it would harm:
     1. the Authority’s reputation; or
     2. the Authority’s interests.
  3. Where the Authority has not:
     1. approved or declined the proposal; or
     2. required further information,

within 20 Working Days of the later of:

* + 1. the date the proposal was first provided to the Authority; or
    2. the date on which further information was provided to the Authority,

then the proposal is, for the purposes of this Contract, approved.

1. Provision of information on Project Specific IPR and Specially Written Software
   1. The Authority may, at any time, require the Supplier to provide information on:
      1. the purposes, other than for the purposes of this Contract, for which the Supplier uses Project Specific IPR and Specially Written Software; and
      2. the activities the Supplier undertakes, other than under this Contract, with or in respect of the Project Specific IPR and Specially Written Software.
   2. The Supplier must provide the information required by the Authority:
      1. within 20 Working Days of the date of the requirement; and
      2. in the form and with the content specified by the Authority.
2. Use of Third Party IPR
   1. The Supplier must not use any:
      1. Third Party Non-COTS Software; or
      2. Third Party Non-COTS Background IPR,

in the provision of the Services (including in any Specially Written Software or in the software element of Project Specific IPRs) unless one of the following conditions is met:

* + 1. the owner or an authorised licensor of the relevant IPR has granted the Authority a direct licence on the terms equivalent to those set out in Paragraph 2.3; or
    2. if the Supplier cannot, after commercially reasonable endeavours, meet the condition in Paragraph 5.1.3, all the following conditions are met:
       1. the Supplier has notified the Authority in writing giving details of:
          1. what licence terms can be obtained from the relevant third party; and
          2. whether there are providers which the Supplier could seek to use and the licence terms obtainable from those third parties;
       2. the Authority approves the licence terms of one of those third parties; and
       3. the owner and authorised licensor of the Third Party IPR has granted a direct licence of the Third Party IPR to the Authority on those terms; or
    3. if the Supplier cannot meet the conditions in Paragraphs 5.1.3 and 5.1.4, the Authority has provided written approval to use the relevant IPR without a licence, with reference to the acts authorised and the specific IPR involved.
  1. The Supplier must not use any:
     1. Third Party COTS Software; or
     2. Third Party COTS Background IPR,

in the provision of the Services (including in any Specially Written Software or in the software element of Project Specific IPRs) unless the following conditions are met:

* + 1. the Supplier has provided the Authority with the applicable terms for the IPRs (which must be at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available); and
    2. the Authority has not (in its absolute discretion) rejected those licence terms within 10 Working Days of the date on which they were provided to the Authority.

1. Licences granted by the Authority
   1. Subject to Paragraph 3, the Authority grants the Supplier a licence to the
      1. the Authority Software;
      2. the Government Data; and
      3. the Authority Background IPRs

that:

* + 1. is perpetual, non-exclusive, royalty-free and non-transferable;
    2. is sub-licensable to any Sub-contractor where:
       1. the Sub-contractor enters into a confidentiality undertaking with the Supplier on the same terms as set out Annex 2 to this Schedule; and
       2. the sub-licence does not purport to provide the sub-licensee with any wider rights than those granted to the Supplier under this Paragraph;
    3. allows the Supplier and any sub-licensee to use, copy and adapt any licensed IPRs for the purpose of:
       1. fulfilling its obligations under this Contract; or
       2. commercially exploiting the Project Specific IPR, the Specially Written Software or the Software Supporting Materials.
  1. When the licence granted under Paragraph 6.1:
     1. terminates in accordance with Paragraph 4; or
     2. no longer has effect at the end of the Term or the expiry of any Termination Assistance Period (whichever is the later),

the Supplier must, and must ensure that each Sub-contractor granted a sub-licence under Paragraph 6.1.5:

* + 1. immediately cease all use of the licensed IPR;
    2. either:
       1. at the discretion of the Authority, return or destroy documents and other tangible materials that contain any of the licensed IPR; or
       2. if the Authority has not made an election within six months of the termination of the licence, destroy the documents and other tangible materials that contain any of the licensed IPR; and
    3. ensure, so far as reasonably practicable, that any licensed IPR held in electronic, digital or other machine-readable form ceases to be readily accessible from any computer, word processor, voicemail system or any other device of the Supplier

***[Guidance:******For Option 5: Supplier rights to all Project Specific IPR and Specially Written Software with royalties, please use the appropriate drafting taken from either Options 2, 3 or Option 4, tailored as appropriate, and include the following additional drafting.]***

## Option 5

1. Royalties
   1. The Supplier must provide a detailed proposal setting out:
      1. the purpose for which it proposes to use the Project Specific IPR, Specially Written Software, the Authority Software, the Government Data and/or the Authority Background IPRs;
      2. the activities the Supplier proposes to undertake with or in respect of the Project Specific IPR, Specially Written Software, the Authority Software, the Government Data and/or the Authority Background IPRs;
      3. its proposed business plan, including:
         1. the goods, services or software to be offered by the Supplier that use or incorporate the Project Specific IPR, Specially Written Software, the Authority Software, the Government Data and/or the Authority Background IPRs;
         2. the relationship between the Project Specific IPR, Specially Written Software, the Authority Software, the Government Data and/or the Authority Background IPRs, and any Supplier Existing IPR or Third Party IPR to be incorporated into, or used to provide, those goods, services or software;
         3. the target markets for those goods, services or software;
         4. the estimated level of orders;
         5. its marketing strategy;
         6. details of the estimated costs, prices, revenues and profits;
         7. the proposed financial benefit to the Authority;
      4. the impact of the proposal on the Services the Supplier provides under the Contract;
      5. an analysis of the likely terms, including financial terms, on which the Supplier would be able to obtain access to intellectual property equivalent to the Project Specific IPR, Specially Written Software, the Authority Software, the Government Data and/or the Authority Background IPRs were it to enter into an arm’s length commercial relationship with a third-party;
      6. the terms on which the Supplier proposes to licence the Authority Software, the Government Data and/or the Authority Background IPRs from the Authority;
      7. any proposed Contract Change; and
      8. any additional agreement the Supplier proposes that it and the Authority enter into;
      9. any other information the Authority requires to properly assess the Supplier’s proposed; and
      10. any other information required by the Authority.
   2. Where the proposed financial benefit to the Authority under Paragraph 1.1.3(g) is, in whole or part, a reduction in the Charges under the Contract, the Supplier must set out how it proposes to apply the revenues and profits received to the Charges payable by the Authority.
   3. Where the Supplier’s proposal provides for the development of new goods, services or software and those goods, services or software are subsequently purchased by the Authority (by whatever means), the terms of that purchase must:
      1. provide for the licencing of the Project Specific IPR and/or the Specially Written Software to the Authority on the same terms as in this Contract; and
      2. include a price that reflects the Charges.
   4. The Supplier acknowledges that:
      1. the Authority may refuse, or require changes to, the Supplier’s proposal in its sole discretion and for any reason; and
      2. in considering the Supplier’s proposal, the Authority must comply with Law relating to:
         1. public procurement; and
         2. subsidy control.
   5. Where the Authority agrees to the Supplier’s proposal, with or without changes, that proposal will not have effect until both Parties have executed:
      1. any additional agreement to give effect to the proposal;
      2. any consequential Contract Change.
   6. Any agreement between the Authority and the Supplier entered into under Paragraph 1.6 must include provisions to the following effect:
      1. the calculation of royalties is based on the following formula:

R = NSV x RR x P

where:

R is the royalty payable on an individual item subject to the agreement;

NSV is the net sales value of the item, that is the price for which the Supplier sold the item to a third party after the deduction of normal trade discounts and excluding Value Added Tax or any other tax or duty based directly on the price of the item and payable by the purchaser;

RR is **[insert:** the royalty payable on the item, expressed as a percentage]; and

P is the proportion that the Project Specific IPR, Specially Written Software, the Authority Software, the Government Data and/or the Authority Background IPRs bears to the whole of the item, expressed as a percentage, subject to the following:

* + - * 1. the proportion that the Project Specific IPR, Specially Written Software, the Authority Software, the Government Data and/or the Authority Background IPRs bears to the item as a whole is an estimation of the effort required to develop the Project Specific IPR, Specially Written Software, the Authority Software, the Government Data and/or the Authority Background IPRs compared to the item as a whole;
        2. P is 100% where, either:

where the proportion of the Project Specific IPR, Specially Written Software, the Authority Software, the Government Data and/or the Authority Background IPRs to the item as a whole is 80% or greater; or

it would not be practicable to create or produce the item without the Project Specific IPR, Specially Written Software, the Authority Software, the Government Data and/or the Authority Background IPRs.

* + 1. all royalties are paid quarterly on the basis of the total sales of the item in that quarter;
    2. each payment of royalties must be accompanied by a detailed statement showing:
       1. the number of items sold in that quarter;
       2. their net sales value; and
       3. the royalties due to the Authority;
    3. the Supplier must keep true and accurate records and books of account containing all information and data necessary for the calculation of royalties, including, for the avoidance of doubt, the calculation of the net sales value and the estimation of P in the formula in Paragraph 1.6
    4. the Supplier must make such books and records available for inspection by the Authority, or the Authority’s representative, whether physically or virtually, at any reasonable time specified by the Authority.

*[Guidance: If using Option 2, please delete the following drafting, as the Supplier does not own the New IPR under that option]:*

1. Clawback
   1. If, within three (3) years of its creation, the Supplier:
      1. is not commercially exploiting any Project Specific IPR or Specially Written Software; or
      2. is not commercially exploiting any Project Specific IPR or Specially Written Software, or is not, to the satisfaction of the Authority, using its best endeavours to do so,

then, on written request from the Authority:

* + - 1. the Supplier must promptly assign to the Authority the Project Specific IPR or Specially Written Software or any specified items of the Project Specific IPR or Specially Written Software; and
      2. the licence to commercially exploit Authority Software, Government Data or Authority Background IPRs terminates either:
      3. on the date specified in the notice; or
      4. where no date is specified in the notice, on the date the notice is received by the Supplier.
  1. Each Party shall bear its own costs of preparing and executing any such assignment.

## Annex 1: Project Specific IPR and Specially Written Software

| Name of Project Specific IPR | Details |
| --- | --- |
|  |  |
|  |  |

| Name of Specially Written Software | Details |
| --- | --- |
|  |  |
|  |  |

| Name of adapted or embedded Supplier Software, Third Party Software, Third Party IPRs, or Supplier Background IPRs | Details |
| --- | --- |
|  |  |
|  |  |

***[Guidance: This may need to be updated throughout the life of the Contract. The Authority should make clear to the Supplier that the Project Specific IPR and Specially Written Software which must be recorded in this Annex does not include all forms of IPR which may be created by the Supplier and the Supplier Staff during the completion of their obligations under the Contract. Only Project Specific IPR and Specially Written Software which is part of a Deliverable, or is necessary for the use of a Deliverable by the Authority will need to be recorded here. IPR such as email communications or documents which do not form part of the Deliverables need not be recorded in this Annex.]***

## Annex 2: Form Of Confidentiality Undertaking

CONFIDENTIALITY AGREEMENT

THIS AGREEMENT is made on [date]

BETWEEN:

1. [insert name] of **[insert** address] (the “Sub-licensee”); and
2. [insert name]of **[insert** address] (the “Supplier” and together with the Supplier, the “Parties”).

WHEREAS:

(A) **[insert** name of Authority] (the “Authority”) and the Supplier are party to a contract dated **[insert** date] (the “Contract”) for the provision by the Supplier of **[insert** brief description of services] to the Authority.

(B) The Authority wishes to grant a sub-licence to the Sub-licensee in respect of certain software and intellectual property rights licensed to the Authority pursuant to the Contract (the “Sub-licence”).

(C) It is a requirement of the Contract that, before the Authority grants such sub-licence to the Sub-licensee, the Sub-licensee execute a confidentiality agreement in favour of the Supplier in or substantially in the form of this Agreement to protect the Confidential Information of the Supplier.

IT IS AGREED as follows:

1. Interpretation
   1. In this Agreement, unless the context otherwise requires:

|  |  |
| --- | --- |
| “Confidential Information” | means:   1. Information, including all personal data within the meaning of the Data Protection Act 2018, and however it is conveyed, provided by the Authority to the Sub-licensee pursuant to or in connection with the Sub-licence that relates to:    1. the Supplier; or    2. the operations, business, affairs, developments, intellectual property rights, trade secrets, know-how and/or personnel of the Supplier; 2. the source code and the object code of the software sub-licensed to the Sub-licensee pursuant to the Sub-licence together with build information, relevant design and development information, technical specifications of all functionality including those not included in standard manuals (such as those that modify system performance and access levels), configuration details, test scripts, user manuals, operating manuals, process definitions and procedures, and all such other documentation supplied by the Supplier to the Authority pursuant to or in connection with the Sub-licence; 3. other Information provided by the Authority pursuant to this Agreement to the Sub-licensee that is clearly designated as being confidential or equivalent or that ought reasonably to be considered to be confidential which comes (or has come) to the Sub-licensee’s attention or into the Sub-licensee’s possession in connection with the Sub-licence; and 4. Information derived from any of the above,   but not including any Information that:   1. was in the possession of the Sub-licensee without obligation of confidentiality prior to its disclosure by the Authority; 2. was already generally available and in the public domain at the time of disclosure otherwise than by a breach of this Agreement or breach of a duty of confidentiality; or 3. was independently developed without access to the Information; |
| “Information” | means all information of whatever nature, however conveyed and in whatever form, including in writing, orally, by demonstration, electronically and in a tangible, visual or machine-readable medium (including CD-ROM, magnetic and digital form); and |
| “Sub-licence” | has the meaning given to that expression in recital 0 to this Agreement. |

* 1. In this Agreement:
     1. a reference to any gender includes a reference to other genders;
     2. the singular includes the plural and vice versa;
     3. the words “include” and cognate expressions shall be construed as if they were immediately followed by the words “without limitation”;
     4. references to any statutory provision include a reference to that provision as modified, replaced, amended and/or re-enacted from time to time (before or after the date of this Agreement) and any prior or subsequent subordinate legislation made under it;
     5. headings are included for ease of reference only and shall not affect the interpretation or construction of this Agreement; and
     6. references to Clauses are to clauses of this Agreement.

1. Confidentiality Obligations
   1. In consideration of the Authority entering into the Sub-licence, the Sub-licensee shall:
      1. treat all Confidential Information as secret and confidential;
      2. have in place and maintain proper security measures and procedures to protect the confidentiality of the Confidential Information (having regard to its form and nature);
      3. not disclose or permit the disclosure of any of the Confidential Information to any other person without obtaining the prior written consent of the Supplier or except as expressly set out in this Agreement;
      4. not transfer any of the Confidential Information outside the United Kingdom;
      5. not use or exploit any of the Confidential Information for any purpose whatsoever other than as permitted under the Sub-licence;
      6. immediately notify the Supplier in writing if it suspects or becomes aware of any unauthorised access, copying, use or disclosure in any form of any of the Confidential Information; and
      7. upon the expiry or termination of the Sub-licence:
         1. destroy or return to the Supplier all documents and other tangible materials that contain any of the Confidential Information;
         2. ensure, so far as reasonably practicable, that all Confidential Information held in electronic, digital or other machine-readable form ceases to be readily accessible (other than by the information technology staff of the Sub-licensee) from any computer, word processor, voicemail system or any other device; and
         3. make no further use of any Confidential Information.
2. Permitted Disclosures
   1. The Sub-licensee may disclose Confidential Information to those of its directors, officers, employees, consultants and professional advisers who:
      1. reasonably need to receive the Confidential Information in connection with the Sub-licence; and
      2. have been informed by the Sub-licensee of the confidential nature of the Confidential Information; and
      3. have agreed to terms similar to those in this Agreement.
   2. The Sub-licensee shall be entitled to disclose Confidential Information to the extent that it is required to do so by applicable law or by order of a court or other public body that has jurisdiction over the Sub-licensee.
   3. Before making a disclosure pursuant to Clause 3.2, the Sub-licensee shall, if the circumstances permit:
      1. notify the Supplier in writing of the proposed disclosure as soon as possible (and if possible before the court or other public body orders the disclosure of the Confidential Information); and
      2. ask the court or other public body to treat the Confidential Information as confidential.
3. General
   1. The Sub-licensee acknowledges and agrees that all property, including intellectual property rights, in Confidential Information disclosed to it by the Supplier shall remain with and be vested in the Supplier.
   2. This Agreement does not include, expressly or by implication, any representations, warranties or other obligations:
      1. to grant the Sub-licensee any licence or rights other than as may be expressly stated in the Sub-licence;
      2. to require the Supplier to disclose, continue disclosing or update any Confidential Information; or
      3. as to the accuracy, efficacy, completeness, capabilities, safety or any other qualities whatsoever of any Information or materials provided pursuant to or in anticipation of the Sub-licence.
   3. The rights, powers and remedies provided in this Agreement are cumulative and not exclusive of any rights, powers or remedies provided by law. No failure or delay by either Party to exercise any right, power or remedy will operate as a waiver of it nor will any partial exercise preclude any further exercise of the same, or of some other right, power or remedy.
   4. Without prejudice to any other rights or remedies that the Supplier may have, the Sub-licensee acknowledges and agrees that damages alone may not be an adequate remedy for any breach by the Sub-licensee of any of the provisions of this Agreement. Accordingly, the Sub-licensee acknowledges that the Supplier shall be entitled to the remedies of injunction and specific performance as well as any other equitable relief for any threatened or actual breach of this Agreement and/or breach of confidence and that no proof of special damages shall be necessary for the enforcement of such remedies.
   5. The maximum liability of the Sub-licensee to the Supplier for any breach of this Agreement shall be limited to ten million pounds (£10,000,000).
   6. For the purposes of the Contracts (Rights of Third Parties) Act 1999 no one other than the Parties has the right to enforce the terms of this Agreement.
   7. Each Party shall be responsible for all costs incurred by it or on its behalf in connection with this Agreement.
   8. This Agreement may be executed in any number of counterparts and by the Parties on separate counterparts, but shall not be effective until each Party has executed at least one counterpart. Each counterpart shall constitute an original of this Agreement, but all the counterparts shall together constitute but one and the same instrument.
4. Notices
   1. Any notice to be given under this Agreement (each a “Notice”) shall be given in writing and shall be delivered by hand and shall be deemed to have been duly given at the time of delivery provided that such Notice is sent to the relevant physical address, and expressly marked for the attention of the relevant individual, set out in Clause 5.2.
   2. Any Notice:
      1. if to be given to the Supplier shall be sent to:

[Address]

Attention: [Contact name and/or position, e.g. “The Finance Director”]

* + 1. if to be given to the Sub-licensee shall be sent to:

[Name of Organisation]  
[Address]

Attention: [ ]

1. Governing law
   1. This Agreement shall be governed by, and construed in accordance with, English law and any matter claim or dispute arising out of or in connection with this Agreement whether contractual or non-contractual, shall be governed by and determined in accordance with English law.
   2. Each Party hereby irrevocably submits to the exclusive jurisdiction of the English courts in respect of any claim or dispute arising out of or in connection with this Agreement.

IN WITNESS of the above this Agreement has been signed by the duly authorised representatives of the Parties on the date which appears at the head of page 1.

For and on behalf of [name of Supplier]

|  |  |
| --- | --- |
| Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Date: |
| Name: | Position: |

For and on behalf of [name of Sub-licensee]

|  |  |
| --- | --- |
| Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Date: |
| Name: | Position: |

Schedule 28

Carbon Reduction

# Schedule 28: Carbon Reduction

1. Definitions
   1. In this Schedule, the following definitions shall apply:

|  |  |
| --- | --- |
| [Optional: "Authority Net Zero Target" | [20XX], being the date by which the Authority commits to achieve Net Zero;] |
| "Carbon Footprint" | the sum of GHG Emissions from an individual, product, organisation or country, measured in tonnes of carbon dioxide-equivalent (t CO2e); |
| "Contract Carbon Footprint" | the GHG Emissions resulting from the execution of the Contract as described by the GHG Protocol Corporate Standard; |
| "Carbon Reduction Plan" or "CRP" | a [Carbon Reduction Plan](https://www.gov.uk/government/publications/procurement-policy-note-0621-taking-account-of-carbon-reduction-plans-in-the-procurement-of-major-government-contracts/guidance-on-adopting-and-applying-ppn-0621-selection-criteria-html) in response to PPN 006; |
| "Emissions Reduction" | the reduction of GHG Emissions from a product, service, contract, organisation or country; |
| "Emissions Reduction Target (ERT)" | the target for Emissions Reduction for each year of the Contract, expressed as a percentage; |
| "Emissions Report" | a report, substantially in the form set out in Table 1, containing, as a minimum, details of the GHG Emissions for this Contract against the Reporting Scopes for each Contract Year, details of any newly identified GHG Hotspots and details of any decarbonisation opportunities; |
| "GHG Emissions Reduction Plan (ERP)" | a plan, substantially in the form set out in Table 2, containing the key activities and interventions that will lead to Emissions Reduction; |
| "Greenhouse Gas Emissions (GHG Emissions)" | the release of greenhouse gases as defined in the GHG Protocol, typically measured in tonnes of carbon dioxide-equivalent (t CO2e); |
| "GHG Hotspots" | processes, operations, and activities that have a proportionately large contribution to the total GHG Emissions for the Contract; |
| "Government Net Zero Target" | the 2050 target date by which the UK government has committed to achieve Net Zero, pursuant to the Climate Change Act 2008 (2050 Target Amendment) Order 2019; |
| "Net Zero" | Net Zero is a state in which the amount of GHG Emissions released into the atmosphere are balanced by the amount of GHG Emissions removed; |
| "Reporting Scopes" | the following categories of GHG Emissions:   * + - 1. "Scope 1 Emissions" are GHG Emissions that come from the Supplier directly, e.g. from burning fuel in vehicles or boilers that the Supplier owns;       2. "Scope 2 Emissions" are GHG Emissions from the Supplier’s use of electricity; and       3. "Scope 3 Emissions" are broken down into 15 sub-categories, including emissions associated with the goods and services you buy, financial services such as investments, and others such as waste or transportation. There are five Scope 3 categories included in the reporting for a Supplier’s CRP: upstream transportation and distribution; waste generated in operations; business travel; employee commuting; and downstream transportation and distribution; and |
| "Supplier Net Zero Target" | the date by which the Supplier commits to achieve Net Zero. |

1. Net Zero Obligation
   1. The Supplier shall, through best endeavours, ensure that their environmental impact is minimised throughout the delivery of the Contract. [**Optional:** The Supplier acknowledges that the Authority has its own operational Authority Net Zero Target of [20xx], and Emissions Reduction achieved in the delivery of this contract will contribute to achieving this aim.]
2. Net Zero Commitment

***[Guidance: The Government Net Zero Target is used to align with the requirements of PPN 016, which requires Suppliers bidding for major government contracts to commit to achieving Net Zero by 2050 and publish a Carbon Reduction Plan.***

***There are two versions of Paragraph 3:***

* ***the first should be included for contracts where a CRP was required as part of the conditions of participation; and***
* ***the second should be included for contracts where a CRP was not required as part of the conditions of participation.***

***Authorities should ensure they include the relevant set and ensure this is consistent with Paragraph 4 below.***

***Paragraph 2 asks the Supplier to acknowledge the Government Net Zero Target and obliges them to set their Supplier Net Zero Target if they haven’t already got one. Where contracts have been in scope of PPN 016, the Supplier will have provided this information as part of their demonstration of compliance with the conditions of participation.***

***If the Supplier did provide a CRP, as PPN 006 requires that the CRP is updated annually, then this requirement will be less burdensome if Authorities can align the reporting dates at points 2.3 and 2.4 to the annual CRP update date.***

***A CRP confirms the Supplier’s commitment to achieving Net Zero by 2050, contains GHG Emissions reported for all required Reporting Scopes and indicates the environmental management measures that the Supplier will be able to apply when performing the contract. For more guidance and a CRP template, please see PPN 006.]***

***[Guidance: This Paragraph should be used where a CRP was required as part of the conditions of participation, delete this Paragraph if not applicable]***

* 1. [**Optional:** The Supplier acknowledges and understands the Government Net Zero Target. Accordingly, and in line with PPN 006, the Supplier shall:
     1. set a Supplier Net Zero Target with a target achievement date the same as or earlier than the Government Net Zero Target;
     2. maintain its Carbon Reduction Plan (CRP) in accordance with PPN 006;
     3. provide details of steps it is taking as an organisation to reduce its Carbon Footprint in the form of Emissions Reduction initiatives; [and]
     4. [**Optional:** where required to do so, undertake and keep up to date full and complete records of GHG Emissions reporting activity undertaken by the Supplier with supporting data and provide the same to the Authority each year; and]
     5. attend, on reasonable notice, meetings with the Authority Representative or other nominated representative to present the Supplier’s CRP to achieve, and current progress towards, the Supplier Net Zero Target [and the Supplier shall refresh its CRP accordingly]].

OR

***[Guidance: This Paragraph should be used where a CRP was not required as part of the conditions of participation, delete this Paragraph if not applicable]***

* 1. [**Optional**: The Supplier acknowledges and understands the Government Net Zero Target. Accordingly, the Supplier shall:
     1. set a Supplier Net Zero Target with a target achievement date the same as or earlier than the Government Net Zero Target;
     2. provide details of any steps it is taking as an organisation to reduce its Carbon Footprint in the form of Emissions Reduction initiatives; [and]
     3. **[Optional:** create a Carbon Reduction Plan, in line with PPN 006, within the first 12 months of contract;]
     4. [**Optional:** where required to do so, undertake and keep up to date full and complete records of GHG Emissions reporting activity undertaken by the Supplier with supporting data and provide the same to the Authority each year; and]
     5. [attend, on reasonable notice, meetings with the Authority Representative or other nominated representative to present the Supplier’s CRP to achieve, and current progress towards, the Supplier Net Zero Target.] [and the Supplier shall refresh its CRP accordingly.]
  2. If the Authority, having reviewed the Emissions Report and discussed with the Supplier its progress to achieve the Supplier Net Zero Target, determines (acting reasonably) that the Supplier is making insufficient progress towards achieving the Supplier Net Zero Date, the Authority may work with the Supplier to determine and implement a suitable rectification plan [in accordance with the Rectification Plan Process].

1. Net Zero Contractual Commitments

***[Guidance: There are three versions of Paragraph 4:***

* ***the first is for Contracts where a CRP was required as part of the conditions of participation;***
* ***the second is for Contracts where a CRP was not required as part of the conditions of participation; and***
* ***the third is for Contracts where a CPR was not required as part of the conditions of participation, but was required by paragraph 3.***

***Authorities should ensure they include the relevant Paragraph and ensure this is consistent with Paragraph 3 above.***

***This section requires the Supplier to set Emissions Reduction targets for the delivery of the Contract (not at an organisational level) and outline specific actions/ behaviours that will be part of the delivery of the Contract.]***

***[Guidance: This Paragraph should be used where a CRP was required as part of the conditions of participation, delete this Paragraph if not applicable.]***

* 1. [**Optional:** The Supplier commits to delivering this Contract in line with its published Carbon Reduction Plan, as per PPN 006, and to support the achievement of the Supplier Net Zero Target and the Government Net Zero Target.]

OR

***[Guidance: This Paragraph should be used where a CRP was not required as part of the conditions of participation, delete this Paragraph if not applicable.]***

* 1. [**Optional**: The Supplier commits to delivering this Contract in a manner which supports the achievement of the Supplier Net Zero Target and the Government Net Zero Target.]

OR

***[Guidance: This Paragraph should be used where a CRP was not required as part of the conditions of participation, but was required by Paragraph 3, delete this Paragraph if not applicable.]***

* 1. [**Optional**: The Supplier commits to delivering this Contract in line with its Carbon Reduction Plan and to support the achievement of the Supplier Net Zero Target and the Government Net Zero Target.
  2. The Supplier shall create a Contract Carbon Footprint by undertaking an assessment of the GHG Emissions for this Contract within [X] months of the Effective Date. The assessment shall aim to quantify the GHG Emissions associated with resources, time and assets deployed in the delivery of the Contract and, in particular, identify GHG Hotspots.

***[Guidance: Alternative specific standards can be referenced here, if more appropriate to the Greenhouse Gas Protocol's Product Standard/ ISO 14064 sector or contract type.]***

* 1. The GHG Emissions assessment outlined in Paragraph 5 should adhere to the [[Greenhouse Gas Protocol's Product Standard](https://ghgprotocol.org/product-standard) / [ISO 14064](https://www.iso.org/standard/66453.html) / **Insert** other standard] and should be conducted to a mutually-agreed level of assurance. The GHG Emissions to be included in the assessment shall be mutually agreed between the Supplier and the Authority.

***[Guidance: 10% is given in Paragraph 4.4 as an indicator. The reduction target will be agreed by the Supplier and the Authority and should be proportionate to the subject matter of the contract and proportionate to its nature, complexity and cost. Authorities may wish to include these considerations as part of their pre-tender market engagement activities.***

***This is the target that will be used to calculate any optional Gain-Share payments due to the Supplier as set out in Paragraph 6.]***

* 1. The Supplier undertakes to, within [X] months of the Effective Date, develop and implement a Carbon Reduction Plan, in the form set out in Table 2, for the Contract, with the objective of reducing the Contract Carbon Footprint of this contract by [10%] per Contract Year throughout the Term (the “**Emissions Reduction Target (ERT)**”), initially focusing on GHG Hotspots and shall update and provide a copy of the Carbon Reduction Plan to the Authority annually.
  2. The Supplier warrants to the Authority that:
     1. it has sufficient resources, infrastructure and materials to achieve the ERT by the date of the expiry of the Contract;
     2. none of the Goods and Services supplied under this Contract will be of lower quality as a result of working towards the ERT; and
     3. it will not offer preferential terms and conditions to those other customers who do not require an ERT or similar obligations in their contracts.

***[Guidance: Paragraph 4.6 requirements should be relevant to the subject matter of the contract and proportionate to its nature, complexity and cost. Authorities may wish to include these considerations as part of their pre-tender market engagement activities.]***

* 1. [**Optional**: At the Authority’s request, the Supplier shall arrange for an independent assessment and verification of the Contract Carbon Footprint. The Supplier shall make a copy of the results available to the Authority as soon as reasonably practicable. The Authority may request this independent assessment no more than once in any period of [two] Contract Years.]

1. Reporting

***[Guidance: Authorities may wish to cross reference Social Value commitments where relevant Reporting Metrics have been used from the Social Value Model.]***

* 1. The Supplier shall:
     1. re-assess the GHG Emissions every Contract Year; and
     2. provide the Authority with a written report of the results of each assessment within [X] months of the completion under Paragraph [4.4] of this Schedule 28 using Table 1: Emissions Report below and every following [X] months. The Authority, acting reasonably, may make adjustments to the content or frequency of Emissions Reports as required.

1. Gain-share

***[Guidance: This section is optional. It should be used to incentivise the Supplier to continue to reduce their Contract Carbon Footprint, even when they’ve reached the annual reduction target. Where this optional section is used, the Authority should consider whether there are any subsidy control implications, which will be contract specific and may need to seek legal advice accordingly.]***

* 1. [Where the Supplier reduces the Contract Carbon Footprint by more than the Emissions Reduction Target percentage stated in Paragraph 4.4 in any one year then the following gain-share mechanism shall apply (“**Gain-Share Mechanism**”):

**Gain-Share Mechanism:**

X = Contract Carbon Footprint in Year 1 (measured in tonnes of CO2e)

Y = Contract Carbon Footprint in Year 2 (measured in tonnes of CO2e). This shall be recorded under “Actual Emissions” in Table 2.

X x % Reduction Target (e.g.10%) = the Emissions Reduction Target expressed in tonnes of CO2e to be achieved in the following year.

Note: The reduction target should be recorded under “Emissions Reduction Target (ERT) (%)” in Table 2.

X – Y = the difference in Contract Carbon Footprint between Previous Year and current Year (measured in tonnes of CO2e). This is known as the “**Actual Emissions Reduction**” (Actual ER).

Actual ER – ERT = “**Additional Emissions Reduction**” for the contract above the agreed [10]% required by Paragraph 4.4 (Additional ER).

Additional ER x 50% of the market rate, as determined by the [UK ETS Authority of the UK Emissions Trading Scheme (UK ETS)](https://www.gov.uk/government/publications/determinations-of-the-uk-ets-carbon-price)\* to offset 1 tonne of CO2e = payment made to the Supplier under the Gain-Share Mechanism (“**Gain-Share Payment**”).

\*As determined by the [UK ETS Authority of the UK Emissions Trading Scheme (UK ETS)](https://www.gov.uk/government/publications/determinations-of-the-uk-ets-carbon-price)]

* 1. The maximum cumulative value of any Gain-Share Payment(s) due to the Supplier in any year of the Contract shall be equal to [up to a maximum of 5]% of the value of the Goods/Services provided by the Supplier to the Authority in respect of that same year.
  2. The Gain-Share Payment shall only become due for payment after any verification process is complete.
  3. The Supplier shall invoice the Authority for any Gain-Share Payment after it has become due for payment and in the absence of any dispute about the level of the Gain-Share Payment it shall be paid by the Authority as if it were part of the Charges.
  4. The Supplier shall invest at least [X]% of any Gain-Share Payment(s) received by the Supplier into green sustainability initiatives. The Authority reserves the right to ask the Supplier for evidence that it is complying with this requirement.]

1. Net Zero Modification
   1. The Parties agree to, wherever possible, perform their obligations under this Contract in a way that minimises the Contract Carbon Footprint associated with the activities under this Contract.

***[Guidance: Paragraphs 7.2-7.7 below set out a modification procedure to reduce the Contract Carbon Footprint. These clauses are intended to be included in contracts which do not already contain an agreed change control procedure. Where the Contract contains a change control procedure, these Paragraphs may be replaced with:***

***“In accordance with the Change Control Procedure, either Party may request or propose a Net Zero modification in the performance of either Party’s obligations under the Contract in order to reduce the Contract Carbon Footprint resulting from this Contract.”]***

* 1. Either Party may serve written notice to the other Party, requesting or proposing a Net Zero modification in the performance of either Party’s obligations under the Contact in order to reduce the Contract Carbon Footprint resulting from this Contract (the “**Net Zero Modification Notice**”).
  2. The Net Zero Modification Notice must outline how the proposal will be implemented and must include:
     1. the reason for the proposed Net Zero modification, including how the modification will assist in delivering the Emissions Reduction Target or, alternatively, how the Net Zero modification will improve the Contract Carbon Footprint;
     2. the time within, and the manner in which, the Supplier proposes to implement the proposed Net Zero modification;
     3. the effect the proposed Net Zero modification will have on delivery of the Contract (including any extension of time required to the date for practical completion); and
     4. any approvals required to implement the proposed Net Zero modification, and the effect of the proposed Net Zero modification on any existing approvals.
  3. The requested Net Zero modification:
     1. must be capable of being implemented within [60] days following agreement between the Parties;
     2. must not result in an increase in an overall liability or cost to either Party or a reduction in the quality of Goods or Services delivered to either Party by the other as contemplated by this Contract; and
     3. must not cause a reduction in compensation due to either Party under the Contract.
  4. Within [X] days of receipt of the Net Zero Modification Notice, the notified Party must provide the notifying Party with a written response either:
     1. accepting the request in the Net Zero Modification Notice [and outlining a way to implement it] within [60] days;
     2. requesting further information; or
     3. rejecting the request in the Net Zero Modification Notice and explaining, reasonably and in good faith;

1. why the request would have a [material] negative impact on the notified party in terms of cost, quality, legal risk, or other relevant factors; or
2. why the request would not have a material impact on reducing the Contract Carbon Footprint resulting from this Contract.
   1. Where the request in the Net Zero Modification Notice is accepted, the contract shall be modified following the Change Control Procedure.
   2. If the notified party rejects the request in the Net Zero Modification Notice in accordance with Paragraph 7.5.3 but the notifying Party does not agree that the request would have a material negative impact on the notified Party then both Parties shall resolve the Dispute in accordance with the Dispute Resolution Procedure.
3. Remediation Plan

***[Guidance: This section is intended to hold the Supplier to account for any failures to meet their Net Zero contractual commitments. The Authority can require the Supplier to implement an improvement plan where it is unlikely to meet its target.]***

* 1. The Supplier shall notify the Authority as soon as it becomes aware of any reason why it might fail to achieve any of the obligations in Paragraph 7. The Authority shall work with the Supplier to agree a remediation plan for the Supplier [in accordance with the Rectification Plan Process].

1. Fuel Emissions

***[Guidance: This Paragraph should be applicable to most contracts, however it should be removed if not relevant to the contract.]***

* 1. The Supplier shall avoid fuel emissions wherever possible by:
     1. arranging meetings using e-conferencing services where face-to-face meetings are not required by the Authority;
     2. using logistics to rationalise journeys and minimise miles travelled in the transportation of goods to Authority Premises;
     3. providing online and webinar-based training for Supplier Staff, minimising the need for travel to attend courses; and
     4. encouraging Supplier Staff to use electric/hybrid vehicles or the rail service rather than petrol, diesel powered vehicles or short haul flights.

1. [Optional Additional Net Zero Paragraphs]

***[Guidance: Authorities will want to include requirements which are appropriate for their Contract, ensuring that these are relevant to the subject matter of the Contract and proportionate and do not create unnecessary burdens upon the Supplier/ supply chain.]***

1. Net Zero Supply Chain Cascade

***[Guidance: This section is optional. If these paragraphs are used, the Authority will want to include requirements which are appropriate for the Contract, ensuring that these are relevant to the subject matter of the Contract and proportionate to its nature, complexity and cost and do not create unnecessary burdens on the Supplier/supply chain.***

***If the contract is related to buildings and infrastructure development then the Authority may want to refer to*** [***PAS2080***](https://www.bsigroup.com/en-GB/products-and-services/assessment-and-certification/product-certification/certify-your-commitment-to-a-more-sustainable-built-environment-carbon-management-in-infrastructure-pas-2080/?creative=685302656329&keyword=pas2080&matchtype=e&network=g&device=c&utm_source=google&utm_medium=cpc&utm_campaign=uk-as-pcert-lg-built-nst-pas2080-builtenvironmentconstruction_bim_sgm-0024&utm_content=685302656329&utm_term=pas2080&adposition=&adgroup=149501117645&gad_source=1&gclid=Cj0KCQiA2KitBhCIARIsAPPMEhJrHPqBneR6zNy_RbG4BSUQdb2-EOFUCVhqpxk2JKrC5-z2oGF63jMaAtT6EALw_wcB)***.***

***The engagement referenced in Paragraph 11.1 could include training, advice on strategy, and sharing best practice on methods of improving sustainability, etc.]***

***[As an alternative to Paragraph 11.1, the Authority may wish to specify in Paragraph 11.2 additional provisions of this Schedule which will be included in Sub-contracts. In doing so, the Authority may give consideration to the impact that this may have on particular Suppliers and how this would impact their procurement. For example, some suppliers are likely to be more sophisticated than others in the carbon reduction initiatives they are able to implement.]***

* 1. [The Supplier shall engage their Sub-contractors to improve their sustainability and encourage them to set their own targets.]
  2. [The Supplier shall ensure that terms equivalent to those set out in Paragraph 2 of this Schedule are included in all Sub-contracts that relate to the Supplier’s obligations under this Contract.]
  3. [The Supplier shall, in line with the Government Net Zero Target [and Authority Net Zero Target] and Emissions Reduction contract targets:
     1. agree responsibilities for Emissions Reduction with Key Sub-contractors; and
     2. map the supply chain and identify critical Sub-contractors].

1. [Optional and Sector Specific Paragraphs]

***[Guidance: Optional and Sector specific Paragraphs can be found in Annex A and should be included here where relevant to the subject matter of the Contract and proportionate.***

***When including these T&Cs please ensure that there is no duplication with any Paragraphs included in other Contract Schedules.]***

1. GHG Emissions Reporting

***[Guidance: All reports and the content of these reports below are optional. The Authority will want to select and amend those reports and requirements which are appropriate for the Contract, ensuring that these are relevant to the subject matter of the Contract and proportionate to its nature, complexity and cost and do not create unnecessary burdens upon the Supplier. Supplier engagement on this is key, as some Suppliers will be more advanced in T&Cs of GHG Emissions reporting than others. For example, where the procurement is not in scope of PPN 006 it may not be appropriate to require the Supplier to report on all Scopes defined in Table 1. If the procurement is in scope of PPN 006 it may only be appropriate to require the Supplier to provide contract Scope 3 emissions for the five categories included in the CRP; however, some Suppliers may be able to provide GHG Emissions reporting for additional categories, or there may be specific categories that are more relevant to the contract.***

***The Authority should test their proposed GHG Emissions reporting requirements with potential Suppliers as part of their preliminary market engagement, and should ensure that GHG Emissions reporting requirements are relevant to the subject matter of the contract and, proportionate to its nature, complexity and cost and do not place undue burdens on Suppliers, especially SME and VCSE Suppliers.***

***The Emissions Report should outline emerging GHG Hotspots and key decarbonisation opportunities for consideration and provide supporting narrative to explain how interventions have affected the results.***

***The Authority should ensure that there is no duplication with other Contract Schedules.]***

Table 1: Emissions Report

| **Contract Year** | **Contract Emissions** | | | **Emerging GHG Hotspots**  **(including narrative to explain how interventions have affected the results)** | **Decarbonisation Opportunities**  **(including narrative to explain how interventions have affected the results)** |
| --- | --- | --- | --- | --- | --- |
| **Scope 1** | **Scope 2** | **Scope 3** |
| **Year 1** |  |  |  |  |  |
| **Year 2** |  |  |  |  |  |
| **Year 3** |  |  |  |  |  |
| **Year 4** |  |  |  |  |  |

Table 2: Carbon Reduction Plan

| **GHG Hotspot** | **Contract Year** | **Estimated Emissions** | **Actual Emissions** | **Emissions Reduction Target (ERT) (%)** | **Actual Reduction (%)** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## Annex A: Optional Paragraphs

***[Guidance: The Optional Paragraphs found in this Annex should be included here where relevant to the subject matter of the Contract and proportionate. When including these T&Cs please ensure that there is no duplication with any Paragraphs included in other Contract Schedules]***

## Part A: General Provisions

1. For the provision and disposal of Goods:
   1. Suppliers should ensure waste is minimised and the amount of waste sent to landfill is reduced. Suppliers should also ensure packaging material is recyclable where possible;
   2. where a Good is unsuitable for refurbishment, the Supplier shall ensure the Good is recycled or disposed of in an environmentally friendly manner;
   3. the Supplier shall provide the Authority with appropriate evidence that the Good has been disposed of in accordance with the requirements of the duty of care for waste as set out in the [Waste Duty of Care Code of Practice 2018,](https://www.gov.uk/government/publications/waste-duty-of-care-code-of-practice) or its successor;
   4. waste materials deposited into landfill sites shall be in accordance with the [Environment Agency Landfill Directive](https://www.gov.uk/guidance/dispose-of-waste-to-landfill);
   5. the Supplier shall work with the Authority to offer a waste management service at little or no cost to the Authority;
   6. where the Supplier stipulates a cost for the waste management service, the Authority shall be provided with a breakdown of all Supplier costs. The Supplier shall detail mitigating action taken to reduce costs for the Authority;
   7. the Supplier shall take responsibility for waste management and work with the Authority to ensure they meet external and internal targets for the reduction of waste. The Supplier shall develop sustainable ways of achieving zero waste to landfill and continuous improvements as advances in technology arise;
   8. the Supplier shall provide information to the Authority on the methods of disposal of waste, showing clear evidence of using disposal methods which are environmentally preferable as required. The Supplier shall, wherever possible, recycle or use for energy recovery to avoid waste being sent to landfill and assure that as much of the waste as possible will be recycled; and
   9. the Authority may request from the Supplier details on the action taken by Supplier to prevent waste being sent to landfill including whether the goods were reused via donation to charitable organisations or good causes.
2. The Supplier shall work proactively with its Sub-contractors to help quantify and reduce the environmental impacts of the Deliverables. When requested by the Authority, the Supplier shall communicate annually on progress and reductions made on the environmental impact of the Deliverables the Supplier has undertaken, in accordance with the terms of the Contract.
3. The Supplier shall deliver the obligations in respect of GHG Emissions reporting requirements, on travel undertaken as part of the delivery of the works and services. GHG Emissions shall be calculated in accordance with the DEFRA guidelines for measuring environmental impacts. The Supplier shall ensure that the version used for calculation is current at the time the figures are produced. The current version may be accessed using the link below: <https://www.gov.uk/government/publications/environmental-reporting-guidelines-including-mandatory-greenhouse-gas-emissions-reporting-guidance>.

## Part B: Sector Specific Paragraphs

1. Technology Sector Paragraphs
   1. The Supplier shall comply with the [EU Data Centres Code of Conduct](https://e3p.jrc.ec.europa.eu/publications/2023-best-practice-guidelines-eu-code-conduct-data-centre-energy-efficiency) (the “**Code of Conduct**”). The Supplier shall ensure that any data centre used in delivering the Services is registered as a “Participant” under this Code of Conduct or provide evidence that the best practices therein have been adopted.
   2. When designing, procuring, implementing and delivering the Contract, the Supplier shall ensure compliance with the [technology code of practice](https://www.gov.uk/guidance/the-technology-code-of-practice#make-your-technology-sustainable), procure “ENERGY STAR” certified products and adopt appropriate best practices set out in ISO 50001 for Energy Management.
2. **IT Hardware Asset Management Sector Paragraphs**
   1. The Supplier shall ensure that IT Assets procured for the delivery of the Contract shall as a minimum comply with Government Buying Standards (“**GBSs**”) where those standards exist for the asset type concerned i.e. laptops, desktops, workstations, scanners and printers.
   2. Where the IT asset is not covered by GBSs the Supplier shall ensure compliance with the GBSs criteria, covering mobile phones, imaging equipment (including printers, scanners, and copiers), and office IT products being monitors/computer displays, personal computers (laptops, notebooks, desktops, thin clients), keyboards, external power supplies and discrete graphic processors.
   3. For asset types where there are no GBSs or EU Green Public Procurement criteria available, the Supplier shall ensure that the models of asset deployed have Energy Star certification (using "ECMA” or equivalent declarations agreed with the Authority) and comply with “EPEAT” or equivalent schemes for sustainable management of resources and energy over the asset lifecycle.
3. **Cloud Services Sector Paragraphs**
   1. When hosting the Services in the cloud, all data centres used either by the Supplier [or by its Sub-contractors] in provision of the Services, must be operated with due regard for energy and cooling efficiency and in accordance with the [EU Data Centres Code of Conduct](https://e3p.jrc.ec.europa.eu/publications/2023-best-practice-guidelines-eu-code-conduct-data-centre-energy-efficiency) (the “**Code**”).
   2. In operation of the cloud service, all available power management facilities on Supplier Assets are to be utilised to deliver the service such that standby and other low power modes are activated to match availability to demand, paying due regard to the Performance Indicators as specified in the Schedule 3 *(Performance Levels)*.
   3. The Supplier shall provide the Authority with a copy of the annual energy return required by the Code, in respect of the energy used in the provision of the Services.
4. **Construction Works Sector Paragraphs**
   1. The Supplier shall, as part of each project contract:
      1. consider and propose methods for designing out waste and designing for destruction;
      2. provide a “Site Waste Management Plan”; and
      3. report on waste performance and, where specified, via an online tool.
   2. The Supplier must adhere to the specific requirements regarding the salvaging of materials, ownership of salvaged materials and storage / removal of salvaged materials. The specific requirements will be defined in each contract.
5. **Facilities Management Sector Paragraphs**
   1. Suppliers shall provide the Authority with a sustainability management plan covering the Suppliers approach to:
      1. energy management;
      2. water, to include system infrastructure maintenance and wastewater management;
      3. waste prevention and management including waste hierarchy and segregation;
      4. recycling of waste paper;
      5. reducing single use plastics in accordance with the [Environmental reporting guidelines: including Streamlined Energy and Carbon Reporting requirements](https://www.gov.uk/government/publications/environmental-reporting-guidelines-including-mandatory-greenhouse-gas-emissions-reporting-guidance) and related Regulations in place across devolved administrations and all future waste related regulations; and
      6. minimising transport use.
   2. The Supplier shall ensure that where they have a responsibility to deliver project works on behalf of the Supplier, all new buildings meet the “BREEAM” or equivalent schemes excellent standard, and that retrofits meet the ‘very good’ standard.
   3. The Supplier shall provide the availability of a professional BREEAM assessor service, provided by licensed BREEAM assessors on all matters relating to the BREEAM assessment of the Authority Premises if required by the Authority including:
      1. reduction in running costs;
      2. measurement and improvement of the performance of Authority Premises;
      3. empowerment of staff;
      4. development of action plans; and
      5. reporting of performance.
   4. Where any new or replacement equipment, to include Assets and component parts which contribute to the Authority's carbon Net Zero performance at the Authority Premises are required, the Supplier shall be responsible for completing “Whole Life Costing” reports, prioritising low-/zero-carbon technologies and ensuring sustainable procurement methods form the basis of the recommendations issued to the Authority. The Supplier shall ensure Authority approval has been received in advance of the commencement of any works at Authority Premises.
   5. All replacement equipment delivered must be new, or (with the Authority’s written approval at its sole discretion) as new if recycled, reconstructed, unused and of recent origin.
   6. The Supplier shall work to reduce the amount of travel undertaken by Supplier Staff and third party Suppliers by combining deliveries of Goods to each Authority Premises.
   7. The Supplier shall work to reduce GHG Emissions from transport by adopting the use of environmentally-friendly transport solutions.
   8. The Supplier shall bring packaging waste in line with UK government initiatives by:
      1. influencing packaging recovery and recycling rates, and so reduce the amount of packaging disposed into landfill; and
      2. Influencing the amount of packaging actually used in the supply chain.
   9. The Supplier shall support energy management initiatives through:
      1. taking account of, and complying with, the Authority’s energy strategy and action plan and its targets under the “Greening Government Commitments” and any subsequent UK government policy;
      2. working with the Authority to meet external and internal targets for reducing energy consumption;
      3. ensuring that all energy-consuming plant under its jurisdiction or control is maintained to operate at optimum efficiency and all fuels, gas, electricity are used economically, in accordance with any operational policies issued by the Authority;
      4. supporting the Authority’s initiatives for energy-saving strategies including separate heating, lighting and ventilation strategies and co-operate with the Authority in achieving agreed objectives; and
      5. for waste management and collection, by:
         1. taking responsibility for waste management and working with the Authority to strive to meet external and internal targets for the reduction of waste and to develop sustainable ways of achieving zero waste to landfill and continuous improvements as advances in technology arise;
         2. providing information to the Authority on the methods of disposal of waste, showing clear evidence of using disposal methods which are environmentally preferable (if required by the Authority). The Supplier shall ensure that as much of the waste as possible will be recycled or used for energy recovery, rather than sent to landfill; and
         3. developing a waste minimisation plan to reduce product consumption by rethinking the need, redeploying, repairing, refurbishing, leasing and/or hiring Assets as appropriate using a formal mobile Asset management plan.
   10. Where a catering Service is provided, the Supplier shall develop a food waste minimisation plan if required by the Authority, in accordance with the best practice standard of the food and catering GBS and with the Waste and Resources Action Programme’s “Hospitality and Food Service Agreement”.
   11. The Supplier shall collect and dispose of all of the waste in line with the “Waste Hierarchy” and best practice.
   12. The Supplier shall ensure that transport GHG Emissions are minimised by optimising collections and ensuring that transportation schedules are planned to reduce GHG Emissions and/or through the use of well maintained, low-emission vehicles and, for example, electric vehicles.
   13. The Supplier shall ensure that all Supplier Staff responsible for collecting waste are trained and adhere to the Authority’s health and safety and environmental policies.
   14. The Supplier shall consider the potential for products to be re-deployed elsewhere, for example, when electrical and electronic products are no longer required, and shall consider using the CCS reuse website for furniture.

Schedule 29

Authority Specific Terms

# Schedule 29: Authority Specific Terms

[Insert Authority Terms]

***[Guidance: HMRC-specific terms will be provided by HMRC]***