Ministry of Housing,
Communities &
Local Government

MHCLG SHORT FORM CONTRACT

PART I INDEX, PART IV SHORT FORM TERMS ("CONDITIONS") & ANNEXES V - X

SHORT FORM CONTRACT FOR THE SUPPLY OF GOODS AND/OR SERVICES

IV. Short form Terms ("Conditions")

1 DFINITIONS USED IN THE CONTRACT

1.1 In this Contract, unless the context otherwise requires, the following words shall have the following meanings:

"Affiliates"	in relation to a body corporate, any other entity which directly or indirectly Controls (in either of the senses defined in sections 450 and 1124 of the Corporation Tax Act 2010 and "**Controlled**" shall be construed accordingly), is Controlled by, or is under direct or indirect common Control of that body corporate from time to time;
"Audit"	the Buyer's right to: (a) verify the accuracy of the Charges and any other amounts payable by the Buyer under the Contract (including proposed or actual variations to them in accordance with the Contract); (b) verify the costs of the Supplier (including the costs of all Subcontractors and any third party suppliers) in connection with the provision of the Deliverables; (c) verify the Supplier's and each Subcontractor's compliance with the applicable Law; (d) identify or investigate actual or suspected breach of clauses 4 to 33 (inclusive), impropriety or accounting mistakes or any breach or threatened breach of security and in these circumstances the Buyer shall have no obligation to inform the Supplier of the purpose or objective of its investigations; (e) identify or investigate any circumstances which may impact upon the financial stability of the Supplier and/or any Subcontractors or their ability to provide the Deliverables; (f) obtain such information as is necessary to fulfil the Buyer's obligations to supply information for parliamentary, ministerial, judicial or administrative purposes including the supply of information to the Comptroller and Auditor General; (g) review any books of account and the internal contract management accounts kept by the Supplier in connection with the Contract; (h) carry out the Buyer's internal and statutory audits and to prepare, examine and/or certify the Buyer's annual and interim reports and accounts; (i) 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 Buyer has used its resources;
"Beneficiary"	a Party having (or claiming to have) the benefit of an indemnity under this Contract;
"Buyer Cause"	has the meaning given to it in the Order Form;
"Buyer"	the person named as Buyer in the Order Form. Where the Buyer is a Crown Body the Supplier shall be treated as contracting with the Crown as a whole;
"Charges"	the charges for the Deliverables as specified in the Order Form;

"Claim"	any claim which it appears that the Buyer is, or may become, entitled to indemnification under this Contract;
"Conditions"	these short form terms and conditions of contract;
"Confidential Information"	all information, whether written or oral (however recorded), provided by the disclosing Party to the receiving Party and which (a) is known by the receiving Party to be confidential; (b) is marked as or stated to be confidential; or (c) ought reasonably to be considered by the receiving Party to be confidential;
"Conflict of Interest"	a direct or indirect conflict between the financial, professional or personal interests of the Supplier or the Supplier Staff and the duties owed to the Buyer under the Contract, in the reasonable opinion of the Buyer;
"Contract"	the contract between the Buyer and the Supplier which is created by the Supplier's counter signing the Order Form and includes the cover letter (if used), Order Form, these Conditions and the Annexes;
"Contract Year"	(a) a period of 12 months commencing on the Start Date; and (b) thereafter a period of 12 months commencing on each anniversary of the Start Date, with the final Contract Year ending on the expiry or termination of the Term;
"Controller"	has the meaning given to it in the UK GDPR or the EU GDPR as the context requires;
"Crown Body"	the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Government and the Welsh Government), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies from time to time carrying out functions on its behalf;
"Data Loss Event"	any event that results, or may result, in unauthorised access to Personal Data held by the Processor 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"	(a) the UK GDPR, (b) the DPA 2018; (c) all applicable Law about the processing of personal data and privacy and guidance issued by the Information Commissioner and other regulatory authority; and (d) (to the extent that it applies) the EU GDPR (and in the event of conflict, the UK GDPR shall apply);
"Data Protection Liability Cap"	has the meaning given to it in row 14 of the Order Form;

"Data Protection Officer"	has the meaning given to it in the UK GDPR or the EU GDPR as the context requires;
"Data Subject Access Request"	a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;
"Data Subject"	has the meaning given to it in the UK GDPR or the EU GDPR as the context requires;
"Deliver"	hand over of the Deliverables to the Buyer at the address and on the date specified in the Order Form, which shall include unloading and stacking and any other specific arrangements agreed in accordance with clause 4.2. "Delivered" and "Delivery" shall be construed accordingly;
"Deliverables"	the Goods, Services, and/or software to be supplied under the Contract as set out in the Order Form;
"Developed System"	the software or system that the Supplier is required to develop under this Contract;
"DPA 2018"	the Data Protection Act 2018;
"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;
"Existing IPR"	any and all intellectual property rights that are owned by or licensed to either Party and which have been developed independently of the Contract (whether prior to the date of the Contract or otherwise);
"Expiry Date"	the date for expiry of the Contract as set out in the Order Form;
"FOIA"	the Freedom of Information Act 2000 together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government department in relation to such legislation;
"Force Majeure Event"	any event, circumstance, matter or cause affecting the performance by either the Buyer or the Supplier of its obligations arising from: (a) acts, events, omissions, happenings or non-happenings beyond the reasonable control of the Party seeking to claim relief in respect of a Force Majeure Event (the **"Affected Party"**) which prevent or materially delay the Affected Party from performing its obligations under the Contract; (b) riots, civil commotion, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare; (c) acts of a Crown Body, local government or regulatory bodies; (d) fire, flood or any disaster; or (e) an industrial dispute affecting a third party for which a substitute third party is not reasonably available but excluding: (a) any industrial dispute relating to the Supplier, the Supplier Staff (including any subsets of them) or any other failure in the Supplier or the Subcontractor's supply chain;

	(b) any event, occurrence, circumstance, matter or cause which is attributable to the wilful act, neglect or failure to take reasonable precautions against it by the Party concerned; and (c) any failure of delay caused by a lack of funds, and which is not attributable to any wilful act, neglect or failure to take reasonable preventative action by that Party;
"Good Industry Practice"	standards, practices, methods and procedures conforming to the Law and the exercise of the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged within the relevant industry or business sector;
"Goods"	the goods to be supplied by the Supplier to the Buyer under the Contract;
"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 Buyer is a, or the, Data Controller; or (c) any meta-data relating to categories of data referred to in (a) or (b) that: (i) is supplied to the Supplier by or on behalf of the Buyer; and/or (ii) that the Supplier is required to generate, Process, Handle, store or transmit under this Contract;
"Indemnifier"	a Party from whom an indemnity is sought under 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 Commissioner"	the UK's independent authority which deals with ensuring information relating to rights in the public interest and data privacy for individuals is met, whilst promoting openness by public bodies;
"Insolvency Event"	in respect of a person: (a) if that person is insolvent; (b) where that person is a company, LLP or a partnership, if an order is made or a resolution is passed for the winding up of the person (other than voluntarily for the purpose of solvent amalgamation or reconstruction); (c) if an administrator or administrative receiver is appointed in respect of the whole or any part of the person's assets or business; (d) if the person makes any composition with its creditors; or (e) takes or suffers any similar or analogous action to any of the actions detailed in this definition as a result of debt in any jurisdiction;
"IP Completion Day"	has the meaning given to it in the European Union (Withdrawal Agreement) Act 2020;
"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;

"Joint Controller Agreement"	the agreement (if any) entered into between the Buyer and the Supplier substantially in the form set out in Part B Joint Controller Agreement *(Optional)* of Annex –1 Processing Personal Data;
"Joint Controllers"	where two or more Controllers jointly determine the purposes and means of processing;
"Key Staff"	any persons specified as such in the Order Form or otherwise notified as such by the Buyer to the Supplier in writing, following agreement to the same by the Supplier;
"Law"	any law, 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;
"Material Breach"	a single serious breach or a number of breaches or repeated breaches (whether of the same or different obligations and regardless of whether such breaches are remedied)
"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 IPR Items"	a deliverable, document, product or other item within which New IPR subsists;
"New IPR"	all and intellectual property rights in any materials created or developed by or on behalf of the Supplier pursuant to the Contract but shall not include the Supplier's Existing IPR;
"Open Licence"	any material that is published for use, with rights to access and modify, 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/ as updated from time to time and the Open Standards Principles documented at https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles as updated from time to time;
"Order Form"	the order form signed by the Buyer and the Supplier printed above these Conditions;
"Party"	the Supplier or the Buyer (as appropriate) and "Parties" shall mean both of them;
"Personal Data Breach"	has the meaning given to it in the UK GDPR or the EU GDPR as the context requires and includes any breach of Data Protection Legislation relevant to Personal Data processed pursuant to the Contract;
"Personal Data"	has the meaning given to it in the UK GDPR or the EU GDPR as the context requires;
"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', 24 November 2016, 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;

"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 the Contract;
"Processor"	has the meaning given to it in the UK GDPR or the EU GDPR as the context requires;
"Protective Measures"	technical and organisational measures which must take account of: (a) the nature of the data to be protected; (b) harm that might result from Data Loss Event; (c) state of technological development; (d) the cost of implementing any measures; including 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 Annex 1 *(Processing Personal Data)* and Annex 6 *(Security Management)* (if used);
"Purchase Order Number" or "PO Number"	the Buyer's unique number relating to the order for Deliverables to be supplied by the Supplier to the Buyer in accordance with the Contract;
"Rectification Plan"	the Supplier's plan (or revised plan) to rectify its Material Breach which shall include: (a) full details of the Material Breach that has occurred, including a root cause analysis; (b) the actual or anticipated effect of the Material Breach; and (c) the steps which the Supplier proposes to take to rectify the Material Breach (if applicable) and to prevent such Material Breach from recurring, including timescales for such steps and for the rectification of the Material Breach (where applicable);
"Request For Information"	has the meaning set out in the FOIA or the Environmental Information Regulations 2004 as relevant (where the meaning set out for the term "**request**" shall apply);
"Security Requirements"	the security requirements set out in the Order Form or in Annex 6 *(Security Management)* (if used);
"Services"	the services to be supplied by the Supplier to the Buyer under the Contract;
"Specification"	the specification for the Deliverables to be supplied by the Supplier to the Buyer (including as to quantity, description and quality) as specified in the Order Form;
"Start Date"	the start date of the Contract set out in the Order Form;
"Sub-Contract"	any contract or agreement (or proposed contract or agreement), other than the Contract, pursuant to which a third party: (a) provides the Deliverables (or any part of them); (b) provides facilities or services necessary for the provision of the Deliverables (or any part of them); and/or

	(c) is responsible for the management, direction or control of the provision of the Deliverables (or any part of them);
"Subcontractor"	any person other than the Supplier, who is a party to a Sub-Contract and the servants or agents of that person;
"Subprocessor"	any third party appointed to process Personal Data on behalf of the Processor related to the Contract;
"Supplier Staff"	any individual engaged, directly or indirectly, or employed by the Supplier or any Subcontractor, in the management or performance of the Supplier's obligations under this Contract;
"Supplier"	the person named as Supplier in the Order Form;
"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 Buyer;
"Term"	the period from the Start Date to the Expiry Date as such period may be extended in accordance with clause 11.2 or terminated in accordance with the Contract;
"Third Party IPR"	intellectual property rights owned by a third party which is or will be used by the Supplier for the purpose of providing the Deliverables;
"Transparency Information"	(a) any information which is published in accordance with guidance issued by His Majesty's Government, from time to time; (b) 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 Buyer, taking into consideration any information which is Confidential Information; and (c) any information about the Contract, including the content of the Contract, and any changes to this Contract agreed from time to time, as well as any information relating to the Deliverables and performance pursuant to the Contract required to be disclosed under FOIA or the Environmental Information Regulations 2004, subject to any exemptions, which shall be determined by the Buyer, taking into consideration any information which is Confidential Information;
"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;
"UK GDPR"	has the meaning as set out in section 3(10) of the DPA 2018, supplemented by section 205(4);
"VAT"	value added tax in accordance with the provisions of the Value Added Tax Act 1994;
"Worker"	any individual that personally performs, or is under an obligation personally to perform services for the Buyer; and
"Working Day"	a day (other than a Saturday or Sunday) on which banks are open for business in the City of London.

2 UNDERSTANDING THE CONTRACT

2.1 In the Contract, unless the context otherwise requires:

2.1.1 references to numbered clauses are references to the relevant clause in these Conditions;

2.1.2 any obligation on any Party not to do or omit to do anything shall include an obligation not to allow that thing to be done or omitted to be done;

2.1.3 references to "writing" include printing, display on a screen and electronic transmission and other modes of representing or reproducing words in a visible form;

2.1.4 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;

2.1.5 the word "including", "for example" and similar words shall be understood as if they were immediately followed by the words "without limitation";

2.1.6 any reference 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) 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 and which 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

2.1.7 a reference to a document (including this Contract) is to that document as varied, amended, novated, ratified or replaced from time to time.

3 HOW THE CONTRACT WORKS

3.1 The Order Form is an offer by the Buyer to purchase the Deliverables subject to and in accordance with the terms and conditions of the Contract.

3.2 The Supplier is deemed to accept the offer in the Order Form when the Buyer receives a copy of the Order Form signed by the Supplier.

3.3 The Supplier warrants and represents that its tender (if any) and all statements made and documents submitted as part of the procurement of Deliverables are and remain true and accurate.

4 WHAT NEEDS TO BE DELIVERED

4.1 All Deliverables

4.1.1 The Supplier must provide Deliverables:

4.1.1.1 in accordance with the Specification, the tender in [Annex 4 – *Supplier* Tender] (Optional) (where applicable) and the Contract;

4.1.1.2 using reasonable skill and care;

4.1.1.3 using Good Industry Practice;

4.1.1.4 using its own policies, processes and internal quality control measures as long as they don't conflict with the Contract;

4.1.1.5 on the dates agreed; and

4.1.1.6 that comply with all Law.

4.1.2 The Supplier must provide Deliverables with a warranty of at least 90 days (or longer where the Supplier offers a longer warranty period to its Buyers) from Delivery against all obvious defects.

4.2 Goods clauses

4.2.1 All Goods delivered must be new, or as new if recycled, unused and of recent origin.

4.2.2 The Supplier transfers ownership of the Goods on completion of Delivery or payment for those Goods, whichever is earlier.

4.2.3 Risk in the Goods transfers to the Buyer on Delivery, but remains with the Supplier if the Buyer notices damage following Delivery and lets the Supplier know within 3 Working Days of Delivery.

4.2.4 The Supplier warrants that it has full and unrestricted ownership of the Goods at the time of transfer of ownership.

4.2.5 The Supplier must Deliver the Goods on the date and to the location specified in the Order Form, during the Buyer's working hours (unless otherwise specified in the Order Form).

4.2.6 The Supplier must provide sufficient packaging for the Goods to reach the point of Delivery safely and undamaged.

4.2.7 All deliveries must have a delivery note attached that specifies the order number, type and quantity of Goods.

4.2.8 The Supplier must provide all tools, information and instructions the Buyer needs to make use of the Goods.

4.2.9 The Supplier will notify the Buyer of any request that Goods are returned to it or the manufacturer after the discovery of safety issues or defects that might endanger health or hinder performance and shall indemnify the Buyer against the costs arising as a result of any such request.

4.2.10 The Buyer can cancel any order or part order of Goods which has not been Delivered. If the Buyer gives less than 14 days' notice then it will pay the Supplier's reasonable and proven costs already incurred on the cancelled order as long as the Supplier takes all reasonable endeavours to minimise these costs.

4.2.11 The Supplier must at its own cost repair, replace, refund or substitute (at the Buyer's option and request) any Goods that the Buyer rejects because they don't conform with clause 4.2. If the Supplier doesn't do this it will pay the Buyer's costs including repair or re-supply by a third party.

4.2.12 The Buyer will not be liable for any actions, claims, costs or expenses incurred by the Supplier or any third party during Delivery of the Goods unless and to the extent that it is caused by negligence or other wrongful act of the Buyer or its servant or agent. If the Buyer suffers or incurs any damage or injury (whether fatal or otherwise) occurring in the course of Delivery or installation then the Supplier shall indemnify the Buyer from any losses, charges, costs or expenses which arise as a result of or in connection with such damage or injury where it is attributable to any act or omission of the Supplier or any of its Subcontractors or Supplier Staff.

4.3 Services clauses

4.3.1 Late Delivery of the Services will be a default of the Contract.

4.3.2 The Supplier must co-operate with the Buyer and third party suppliers on all aspects connected with the delivery of the Services and ensure that Supplier Staff comply with any reasonable instructions including the Security Requirements (where any such requirements have been provided).

4.3.3 The Buyer must provide the Supplier with reasonable access to its premises at reasonable times for the purpose of supplying the Services

4.3.4 The Supplier must at its own risk and expense provide all equipment required to deliver the Services. Any equipment provided by the Buyer to the Supplier for supplying the Services remains the property of the Buyer and is to be returned to the Buyer on expiry or termination of the Contract.

4.3.5 The Supplier must allocate sufficient resources and appropriate expertise to the Contract.

4.3.6 The Supplier must take all reasonable care to ensure performance does not disrupt the Buyer's operations, employees or other contractors.

4.3.7 On completion of the Services, the Supplier is responsible for leaving the Buyer's premises in a clean, safe and tidy condition and making good any damage that it has caused to the Buyer's premises or property, other than fair wear and tear.

4.3.8 The Supplier must ensure all Services, and anything used to deliver the Services, are of good quality and free from defects.

4.3.9 The Buyer is entitled to withhold payment for partially or undelivered Services, but doing so does not stop it from using its other rights under the Contract.

5 PRICING AND PAYMENTS

5.1 In exchange for the Deliverables, the Supplier must invoice the Buyer for the charges in the Order Form.

5.2 All Charges:

5.2.1 exclude VAT, which is payable on provision of a valid VAT invoice; and

5.2.2 include all costs and expenses connected with the supply of Deliverables.

5.3 The Buyer must pay the Supplier the charges:

5.3.1 within 30 days beginning with the day on which an invoice is received by the Buyer in respect of the sum, or

5.3.2 if later, the day by which the payment falls due in accordance with the invoice,

subject to the invoice being verified as valid and undisputed.

5.4 A Supplier invoice is only valid if it:

5.4.1 includes the minimum required information set out in Section 88(7) of the Procurement Act 2023;

5.4.2 includes all appropriate references including the Purchase Order Number and other details reasonably requested by the Buyer; and

5.4.3 includes a detailed breakdown of Deliverables which have been delivered.

5.5 If there is a dispute between the Parties as to the amount invoiced, the Buyer shall pay the undisputed amount. The Supplier shall not suspend the provision of the Deliverables unless the Supplier is entitled to terminate the Contract for a failure to pay undisputed sums in accordance with clause 11.6. Any disputed amounts shall be resolved through the dispute resolution procedure detailed in clause 35.

5.6 The Buyer may retain or set-off payment of any amount owed to it by the Supplier under this Contract or any other agreement between the Supplier and the Buyer if notice and reasons are provided.

5.7 The Supplier must ensure that all Subcontractors are paid, in full:

5.7.1 within 30 days beginning with the day on which an invoice is received by the Buyer in respect of the sum; or

5.7.2 if later, the date by which the payment falls due in accordance with the invoice,

subject to the invoice being verified as valid and undisputed.

5.8 If the invoice is not paid in accordance with the timescales in clause 5.7, the Buyer can publish the details of the late payment or non-payment.

5.9 Where any invoice does not conform to the Buyer's requirements set out in clause 5.4, or the Buyer disputes the invoice, the Buyer shall notify the Supplier without undue delay and the Supplier shall promptly issue a replacement invoice which shall comply with such requirements.

6 THE BUYER'S OBLIGATIONS TO THE SUPPLIER

6.1 If Supplier fails to comply with the Contract as a result of a Buyer Cause:

6.1.1 the Buyer cannot terminate the Contract under clause 11;

6.1.2 the Supplier is entitled to reasonable and proven additional expenses and to relief from liability under this Contract;

6.1.3 the Supplier is entitled to additional time needed to deliver the Deliverables; and

6.1.4 the Supplier cannot suspend the ongoing supply of Deliverables.

6.2 Clause 6.1 only applies if the Supplier:

6.2.1 gives notice to the Buyer within 10 Working Days of becoming aware;

6.2.2 demonstrates that the failure only happened because of the Buyer Cause; and

6.2.3 mitigated the impact of the Buyer Cause.

7 RECORD KEEPING AND REPORTING

7.1 The Supplier must ensure that suitably qualified representatives attend progress meetings with the Buyer and provide progress reports when specified in the Order Form.

7.2 The Supplier must keep and maintain full and accurate records and accounts on everything to do with the Contract for 7 years after the date of expiry or termination of the Contract and in accordance with the UK GDPR or the EU GDPR as the context requires.

7.3 The Supplier must allow any auditor appointed by the Buyer access to its premises to verify all contract accounts and records of everything to do with the Contract and provide copies for the Audit.

7.4 The Buyer or an auditor can Audit the Supplier.

7.5 During an Audit, the Supplier must provide information to the auditor and reasonable co-operation at their request.

7.6 The Parties will bear their own costs when an Audit is undertaken unless the Audit identifies a Material Breach by the Supplier, in which case the Supplier will repay the Buyer's reasonable costs in connection with the Audit.

7.7 If the Supplier is not providing any of the Deliverables, or is unable to provide them, it must immediately:

7.7.1 tell the Buyer and give reasons;

7.7.2 propose corrective action; and

7.7.3 provide a deadline for completing the corrective action.

7.8 If the Buyer, acting reasonably, is concerned as to the financial stability of the Supplier such that it may impact on the continued performance of the Contract then the Buyer may:

7.8.1 require that the Supplier provide to the Buyer (for its approval) a plan setting out how the Supplier will ensure continued performance of the Contract and the Supplier will make changes to such plan as reasonably required by the Buyer and once it is agreed then the Supplier shall act in accordance with such plan and report to the Buyer on demand; and

7.8.2 if the Supplier fails to provide a plan or fails to agree any changes which are requested by the Buyer or fails to implement or provide updates on progress with the plan, terminate the Contract immediately for Material Breach (or on such date as the Buyer notifies) and the consequences of termination in clause 11.5.1 shall apply.

7.9 If there is a Material Breach, the Supplier must notify the Buyer within 3 Working Days of the Supplier becoming aware of the Material Breach. The Buyer may request that the Supplier provide a Rectification Plan within 10 Working Days of the Buyer's request alongside any additional documentation that the Buyer requires. Once such Rectification Plan is agreed between the

Parties (without the Buyer limiting its rights) the Supplier must immediately start work on the actions in the Rectification Plan at its own cost.

7.10 At the end of each Contract Year, at its own expense, the Supplier will provide a report to the Buyer setting out a summary of its compliance with clause 5.7, such report to be certified by the Supplier's Authorised Representative as being accurate and not misleading.

8 SUPPLIER STAFF

8.1 The Supplier Staff involved in the performance of the Contract must:

8.1.1 be appropriately trained and qualified;

8.1.2 be vetted in accordance with the Buyer's staff vetting procedures as specified in the Order Form or in Annex 6 *(Security Requirements)* (if used); and

8.1.3 comply with all conduct requirements when on the Buyer's premises.

8.2 Where the Buyer decides one of the Supplier's Staff isn't suitable to work on the Contract, the Supplier must replace them with a suitably qualified alternative.

8.3 The Supplier must provide a list of Supplier Staff needing to access the Buyer's premises and say why access is required.

8.4 The Supplier indemnifies the Buyer against all claims brought by any person employed or engaged by the Supplier caused by an act or omission of the Supplier or any Supplier Staff.

8.5 The Buyer indemnifies the Supplier against all claims brought by any person employed or engaged by the Buyer caused by an act or omission of the Buyer or any of the Buyer's employees, agents, consultants and contractors.

8.6 The Supplier shall use those persons nominated (if any) as Key Staff in the Order Form or otherwise notified as such by the Buyer to the Supplier in writing, following agreement to the same by the Supplier to provide the Deliverables and shall not remove or replace any of them unless:

8.6.1 requested to do so by the Buyer or the Buyer approves such removal or replacement (not to be unreasonably withheld or delayed);

8.6.2 the person concerned resigns, retires or dies or is on parental or long-term sick leave; or

8.6.3 the person's employment or contractual arrangement with the Supplier or any Subcontractor is terminated for material breach of contract by the employee.

8.7 The Supplier shall ensure that no person who discloses that they have a conviction that is relevant to the nature of the Contract, relevant to the work of the Buyer, or is of a type otherwise advised by the Buyer (each such conviction a "**Relevant Conviction**"), or is found by the Supplier to have a Relevant Conviction (whether as a result of a police check, a disclosure and barring service check or otherwise) is employed or engaged in the provision of any part of the Deliverables.

9 RIGHTS AND PROTECTION

9.1 The Supplier warrants and represents that:

9.1.1 it has full capacity and authority to enter into and to perform the Contract;

9.1.2 the Contract is entered into by its authorised representative;

9.1.3 it is a legally valid and existing organisation incorporated in the place it was formed;

9.1.4 there are no known legal or regulatory actions or investigations before any court, administrative body or arbitration tribunal pending or threatened against it or its affiliates that might affect its ability to perform the Contract;

9.1.5 all necessary rights, authorisations, licences and consents (including in relation to IPRs) are in place to enable the Supplier to perform its obligations under the Contract and the Buyer to receive the Deliverables;

9.1.6 it doesn't have any contractual obligations which are likely to have a material adverse effect on its ability to perform the Contract; and

9.1.7 it is not impacted by an Insolvency Event.

9.2 The warranties and representations in clause 3.3 and clause 9.1 are repeated each time the Supplier provides Deliverables under the Contract.

9.3 The Supplier indemnifies the Buyer against each of the following:

9.3.1 wilful misconduct of the Supplier, any of its Subcontractor and/or Supplier Staff that impacts the Contract; and

9.3.2 non-payment by the Supplier of any tax or National Insurance.

9.4 If the Supplier becomes aware of a representation or warranty made in relation to the Contract that becomes untrue or misleading, it must immediately notify the Buyer.

9.5 All third party warranties and indemnities covering the Deliverables must be assigned for the Buyer's benefit by the Supplier for free.

10 INTELLECTUAL PROPERTY RIGHTS ("IPRS")

10.1 Each Party keeps ownership of its own Existing IPRs. The Supplier gives the Buyer a non-exclusive, perpetual, royalty-free, irrevocable, transferable, sub-licensable worldwide licence to use, copy and adapt the Supplier's Existing IPR to enable the Buyer and its sub-licensees to both:

10.1.1 receive and use the Deliverables; and

10.1.2 use the New IPR.

The termination or expiry of the Contract does not terminate any licence granted under this clause 10.

10.2 Any New IPR created under the Contract is owned by the Buyer. The Buyer gives the Supplier a royalty-free, non-exclusive, non-transferable licence to use, copy, and adapt any Existing IPRs and the New IPR which the Supplier reasonably requires for the purpose of fulfilling its obligations during the Term and commercially exploiting the New IPR developed under the Contract. This licence is sub-licensable to a Subcontractor for the purpose of enabling the Supplier to fulfil its obligations under the Contract, and in that case the Subcontractor must enter into a confidentiality undertaking with the Supplier on the same terms as set out in clause 15 (What you must keep confidential).

10.3 Unless otherwise agreed in writing, the Supplier and the Buyer will record any New IPR and keep this record updated throughout the Term.

10.4 Where a Party acquires ownership of intellectual property rights incorrectly under this Contract, it must do everything reasonably necessary to complete a transfer assigning them in writing to the other Party on request and at its own cost.

10.5 Neither Party has the right to use the other Party's intellectual property rights, including any use of the other Party's names, logos or trademarks, except as provided in this clause 10 or otherwise agreed in writing.

10.6 If any claim is made against the Buyer for actual or alleged infringement of a third party's intellectual property arising out of, or in connection with, the supply or use of the Deliverables (an "**IPR Claim**"), then the Supplier indemnifies the Buyer against all losses, damages, costs or expenses (including professional fees and fines) incurred as a result of the IPR Claim.

10.7 If an IPR Claim is made or anticipated, the Supplier must at its own option and expense, either:

10.7.1 obtain for the Buyer the rights in clause 10.1 without infringing any third-party intellectual property rights; and

10.7.2 replace or modify the relevant item with substitutes that don't infringe intellectual property rights without adversely affecting the functionality or performance of the Deliverables.

10.7.3 If the Supplier is not able to resolve the IPR Claim to the Buyer's reasonable satisfaction within a reasonable time, the Buyer may give written notice that it terminates the Contract from the date set out in the notice, or where no date is given in

the notice, the date of the notice. On termination, the consequences of termination in clause 11.5.1 shall apply.

10.8 The Supplier shall not use in the Delivery of the Deliverables any Third Party IPR unless:

10.8.1 the Buyer gives its approval to do so; and

10.8.2 one of the following conditions applies:

10.8.2.1 the owner or an authorised licensor of the relevant Third Party IPR has granted the Buyer a direct licence that provides the Buyer with the rights in clause 10.1; or

10.8.2.2 if the Supplier cannot, after commercially reasonable endeavours, obtain for the Buyer a direct licence to the Third Party IPR as set out in clause 10.8.2.1:

(a) the Supplier provides the Buyer with details of the licence terms it can obtain and the identity of those licensors;

(b) the Buyer agrees to those licence terms; and

(c) the owner or authorised licensor of the Third Party IPR grants a direct licence to the Buyer on those terms; or

10.8.2.3 the Buyer approves in writing, with reference to the acts authorised and the specific intellectual property rights involved.

10.9 In spite of any other provisions of the Contract and for the avoidance of doubt, award of this Contract by the Buyer and the ordering of any Deliverable under it, does not constitute an authorisation by the Crown under Sections 55 and 56 of the Patents Act 1977, Section 12 of the Registered Designs Act 1949 or Sections 240 – 243 of the Copyright, Designs and Patents Act 1988.

11 ENDING THE CONTRACT

11.1 The Contract takes effect on the Start Date and ends on the earlier of the Expiry Date or termination of the Contract, or earlier if required by Law.

11.2 The Buyer can extend the Contract where set out in the Order Form in accordance with the terms in the Order Form.

11.3 Ending the Contract without a reason

The Buyer has the right to terminate the Contract at any time without reason or liability by giving the Supplier not less than 90 days' written notice, and if it's terminated clause 11.6.2 applies.

11.4 When the Buyer can end the Contract

11.4.1 If any of the following events happen, the Buyer has the right to immediately terminate its Contract by issuing a termination notice in writing to the Supplier and the consequences of termination in clause 11.5.1 shall apply:

11.4.1.1 there's a Supplier Insolvency Event;

11.4.1.2 the Supplier is in Material Breach of the Contract;

11.4.1.3 there's a change of control (within the meaning of section 450 of the Corporation Tax Act 2010) of the Supplier which isn't pre-approved by the Buyer in writing;

11.4.1.4 the Supplier or its affiliates embarrass or bring the Buyer into disrepute or diminish the public trust in them; or

11.4.1.5 the Supplier fails to comply with its legal obligations in the fields of environmental, social or employment Law when providing the Deliverables.

11.5 What happens if the Contract ends

11.5.1 Where the Buyer terminates the Contract under clause 10.7.3, 11.4, 7.8.2, 32.4 or Paragraph 8 of Part B Joint Controller Agreement *(Optional)* of Annex –1 Processing Personal Data (if used), all of the following apply:

11.5.1.1 the Supplier is responsible for the Buyer's reasonable costs of procuring replacement Deliverables for the rest of the term of the Contract;

11.5.1.2 the Buyer's payment obligations under the terminated Contract stop immediately;

11.5.1.3 accumulated rights of the Parties are not affected;

11.5.1.4 the Supplier must promptly delete or return the Government Data other than Government Data (i) that is Personal Data in respect of which the Supplier is a Controller; (ii) in respect of which the Supplier has rights to hold the Government Data independently of this Contract; and (iii) where required to retain copies by Law;

11.5.1.5 the Supplier must promptly return any of the Buyer's property provided under the Contract;

11.5.1.6 the Supplier must, at no cost to the Buyer, give all reasonable assistance to the Buyer and any incoming supplier and co-operate fully in the handover and re-procurement; and

11.5.1.7 the Supplier must repay to the Buyer all the Charges that it has been paid in advance for Deliverables that it has not provided as at the date of termination or expiry.

11.5.2 The following clauses survive the expiry or termination of the Contract: IV, 4.2.9, 5, 7, 8.4, 10, 11.5, 11.6.2, 12, 14, 15, 16, 18, 19, 22, 31.2.2, 35 and 36 and any clauses which are expressly or by implication intended to continue.

11.6 When the Supplier can end the Contract and what happens when the contract ends (Buyer and Supplier termination)

11.6.1 The Supplier can issue a reminder notice if the Buyer does not pay an undisputed invoice on time. The Supplier can terminate the Contract if the Buyer fails to pay an undisputed invoiced sum due and worth over 10% of the total Contract value or £1,000, whichever is the lower, within 30 days of the date of the reminder notice.

11.6.2 Where the Buyer terminates the Contract in accordance with clause 11.3 or the Supplier terminates the Contract under clause 11.6 or 23.4:

11.6.2.1 the Buyer must promptly pay all outstanding charges incurred by the Supplier;

11.6.2.2 the Buyer must pay the Supplier reasonable committed and unavoidable losses as long as the Supplier provides a fully itemised and costed schedule with evidence - the maximum value of this payment is limited to the total sum payable to the Supplier if the Contract had not been terminated; and

11.6.2.3 clauses 11.5.1.2 to 11.5.1.7 apply.

11.6.3 The Supplier also has the right to terminate the Contract in accordance with clauses 20.3 and 23.4.

11.7 Partially ending and suspending the Contract

11.7.1 Where the Buyer has the right to terminate the Contract it can terminate or suspend (for any period), all or part of it. If the Buyer suspends the Contract it can provide the Deliverables itself or buy them from a third party.

11.7.2 The Buyer can only partially terminate or suspend the Contract if the remaining parts of it can still be used to effectively deliver the intended purpose.

11.7.3 The Parties must agree (in accordance with clause 25) any necessary variation required by clause 11.7, but the Supplier may not either:

11.7.3.1 reject the variation; or

11.7.3.2 increase the Charges, except where the right to partial termination is under clause 11.3.

11.7.4 The Buyer can still use other rights available, or subsequently available to it if it acts on its rights under clause 11.7.

12 HOW MUCH YOU CAN BE HELD RESPONSIBLE FOR

12.1 Each Party's total aggregate liability under or in connection with the Contract (whether in tort, contract or otherwise) is no more than 125% of the Charges paid or payable to the Supplier.

12.2 No Party is liable to the other for:

12.2.1 any indirect losses; and/or

12.2.2 loss of profits, turnover, savings, business opportunities or damage to goodwill (in each case whether direct or indirect).

12.3 In spite of clause 12.1, neither Party limits or excludes any of the following:

12.3.1 its liability for death or personal injury caused by its negligence, or that of its employees, agents or Subcontractors;

12.3.2 its liability for bribery or fraud or fraudulent misrepresentation by it or its employees; or

12.3.3 any liability that cannot be excluded or limited by Law.

12.4 In spite of clause 12.1, the Supplier does not limit or exclude its liability for any indemnity given under clauses 8.4, 9.3.2, 10.6, or 31.2.2.

12.5 In spite of clause 12.1, the Buyer does not limit or exclude its liability for any indemnity given under clause 8.5.

12.6 In spite of clause 12.1, but subject to clauses 12.2 and 12.3, the Supplier's total aggregate liability in each Contract Year under clause 14.6.4 is no more than the Data Protection Liability Cap.

12.7 Each Party must use all reasonable endeavours to mitigate any loss or damage which it suffers under or in connection with the Contract, including any indemnities.

12.8 If more than one Supplier is party to the Contract, each Supplier Party is fully responsible for both their own liabilities and the liabilities of the other Suppliers.

13 OBEYING THE LAW

13.1 The Supplier, in connection with provision of the Deliverables:

13.1.1 is expected to meet and have its Subcontractors meet the standards set out in the Supplier Code of Conduct: (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1163536/Supplier_Code_of_Conduct_v3.pdff) as such Code of Conduct may be updated from time to time, and such other sustainability requirements as set out in the Order Form. The Buyer also expects to meet this Code of Conduct;

13.1.2 must comply with the provisions of the Official Secrets Acts 1911 to 1989 and section 182 of the Finance Act 1989;

13.1.3 must support the Buyer in fulfilling its Public Sector Equality duty under section 149 of the Equality Act 2010;

13.1.4 must comply with the model contract terms contained in (a) to (l) of Annex C of the guidance to PPN 009 (Tackling Modern Slavery in Government Supply Chains), as such clauses may be amended or updated from time to time; and

13.1.5 meet the applicable Government Buying Standards applicable to Deliverables which can be found online at: https://www.gov.uk/government/collections/sustainable-procurement-the-government-buying-standards-gbs, as updated from time to time.

13.2 The Supplier indemnifies the Buyer against any costs resulting from any default by the Supplier relating to any applicable Law to do with the Contract.

13.3 The Supplier must appoint a compliance officer who must be responsible for ensuring that the Supplier complies with Law, clause 13.1 and clauses 27 to 33.

14 DATA PROTECTION AND SECURITY

14.1 The Supplier must not remove any ownership or security notices in or relating to the Government Data.

14.2 The Supplier must ensure that any Supplier, Subcontractor, or Sub-processor system holding any Government Data, including back-up data, is a secure system that complies with the Security Requirements (including Annex 6 *(Security Management)* (if used)) or as otherwise provided in writing by the Buyer (where any such requirements have been provided).

14.3 The Supplier must not store, copy, disclose, or use the Government Data except as necessary for the performance by the Supplier of its obligations under this Contract or as otherwise expressly authorised in writing by the Buyer, other than Government Data which is Personal Data in respect of which the Supplier is a Controller, or the Supplier has rights to hold the Government Data independently of the Contract.

14.4 If at any time the Supplier suspects or has reason to believe that the Government Data is corrupted, lost or sufficiently degraded, then the Supplier must immediately notify the Buyer and suggest remedial action.

14.5 If the Government Data is any of (i) corrupted, (ii) lost or (iii) sufficiently degraded, in each case as a result of the Supplier's Default, so as to be unusable the Buyer may either or both:

14.5.1 tell the Supplier (at the Supplier's expense) to restore or get restored Government Data as soon as practical but no later than 5 Working Days from the date that the Buyer receives notice, or the Supplier finds out about the issue, whichever is earlier; and/or

14.5.2 restore the Government Data itself or using a third party and shall be repaid by the Supplier any reasonable expenses incurred in doing so.

14.6 The Supplier:

14.6.1 must, subject to the Security Requirements (if any), provide the Buyer with all Government Data in an agreed format (provided it is secure and readable) within 10 Working Days of a written request;

14.6.2 must have documented processes to guarantee prompt availability of Government Data if the Supplier stops trading;

14.6.3 must, subject to the Security Requirements (if any), securely erase (using a deletion method that ensures that even a determined expert using specialist techniques can recover only a small fraction of the data deleted) all Government Data and any copies it or a Subcontractor holds when asked to do so by the Buyer unless required by Law to retain it, other than in relation to Government Data in respect of which the Supplier is a Controller or which the Supplier has rights to hold the Government Data independently of this Contract; and

14.6.4 indemnifies the Buyer against any and all losses incurred if the Supplier breaches clause 14 or any Data Protection Legislation.

14.7 The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under the Contract dictates the status of each party under the DPA 2018. A Party may act as:

14.7.1 "Controller" in respect of the other Party who is "Processor";

14.7.2 "Processor" in respect of the other Party who is "Controller";

14.7.3 "Joint Controller" with the other Party;

14.7.4 "Independent Controller" of the Personal Data where the other Party is also "Controller",

in respect of certain Personal Data under the Contract and shall specify in Part A Authorised Processing Template of Annex –1 Processing Personal Data which scenario they think shall apply in each situation.

14.8 Where one Party is Controller and the other Party its Processor

14.8.1 Where a Party is a Processor, the only processing that the Processor is authorised to do is listed in Part A Authorised Processing Template of Annex –1 Processing Personal Data by the Controller and may not be determined by the Processor. The term "processing" and any associated terms are to be read in accordance with Article 4 of the UK GDPR and EU GDPR (as applicable).

14.8.2 The Processor must notify the Controller immediately if it thinks the Controller's instructions breach the Data Protection Legislation.

14.8.3 The Processor must give all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment before starting any processing, which may include, at the discretion of the Controller:

14.8.3.1 a systematic description of the expected processing and its purpose;

14.8.3.2 the necessity and proportionality of the processing operations;

14.8.3.3 the risks to the rights and freedoms of Data Subjects; and

14.8.3.4 the intended measures to address the risks, including safeguards, security measures and mechanisms to protect Personal Data and assurance that those measures comply with any Security Requirements.

14.8.4 The Processor must, in in relation to any Personal Data processed under this Contract:

14.8.4.1 process that Personal Data only in accordance with this clause 14, Part A Authorised Processing Template of Annex –1 Processing Personal Data and Annex 6 *(Security Management)* (if used), unless the Processor is required to do otherwise by Law. If lawful to notify the Controller, the Processor must promptly notify the Controller if the Processor is otherwise required to process Personal Data by Law before processing it.

14.8.4.2 put in place appropriate Protective Measures to protect against a Data Loss Event which must be approved by the Controller.

14.8.4.3 ensure that:

(a) the Processor Personnel do not process Personal Data except in accordance with clause 14, Part A Authorised Processing Template of Annex –1 Processing Personal Data and Annex 6 *(Security Management)* (if used);

(b) it uses the Buyer's staff vetting procedures to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

i. are aware of and comply with the Processor's duties under this clause 14 and Annex 6 *(Security Management)* (if used);

ii. are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;

iii. are informed of the confidential nature of the Personal Data and do not provide any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise allowed by the Contract; and

iv. have undergone adequate training in the use, care, protection and handling of Personal Data.

(c) the Processor must not transfer Personal Data outside of the UK and/or the EEA unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

i. the transfer is in accordance with Article 45 of the UK GDPR (or section 74A of DPA 2018) 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 Subcontractors and/or Subprocessors), the Supplier (and/or the applicable Subcontractor and/or Subprocessor) must be self-certified and continue to be self-certified on the US Data Privacy Framework;

(B) the Supplier shall notify the Buyer immediately if there are any, or there are reasonable grounds to believe there may be any, changes in respect of their and/or their Subcontractor's or Subprocessor'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 clause 14.8.4.3(c)i; and

(C) in the event that the Supplier (and/or the applicable Subcontractor or Subprocessor):

(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 clause 14.8.4.3(c)i;

(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 clause 14.8.4.3(c)i; and/or

(3) fails to notify the Buyer of any changes to its certification status in accordance with clause 14.8.4.3(c)i(B) above,

the Buyer shall have the right to terminate this Contract with immediate effect; or

(d) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or section 75 of the DPA 2018) and/or the transfer is in accordance with Article 46 of the EU GDPR (where applicable) as determined by the Controller which could include relevant parties entering into:

i. where the transfer is subject to UK GDPR:

(A) the International Data Transfer Agreement (the "**IDTA**"), as published by the Information Commissioner's Office from time to time under section 119A(1) of the DPA 2018 as well as any additional measures determined by the Controller;

(B) 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 ("**EU SCCs**"), together with the UK International Data Transfer Agreement Addendum to the EU SCCs (the "**Addendum**") as published by the Information Commissioner's Office from time to time; and/or

ii. 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;

(e) the Data Subject has enforceable rights and effective legal remedies when transferred;

(f) the Processor meets its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; and

(g) the Processor complies with the Controller's reasonable prior instructions about the processing of the Personal Data.

14.8.5 The Processor must at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.

14.8.6 The Processor must notify the Controller immediately if it:

14.8.6.1 receives a Data Subject Access Request (or purported Data Subject Access Request);

14.8.6.2 receives a request to rectify, block or erase any Personal Data;

14.8.6.3 receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

14.8.6.4 receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Contract;

14.8.6.5 receives a request from any third Party for disclosure of Personal Data where compliance with the request is required or claims to be required by Law; and

14.8.6.6 becomes aware of a Data Loss Event.

14.8.7 Any requirement to notify under clause 14.8.6 includes the provision of further information to the Controller in stages as details become available.

14.8.8 The Processor must promptly provide the Controller with full assistance in relation to any Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 14.8.6. This includes giving the Controller:

14.8.8.1 full details and copies of the complaint, communication or request;

14.8.8.2 reasonably requested assistance so that it can comply with a Data Subject Access Request within the relevant timescales in the Data Protection Legislation;

14.8.8.3 any Personal Data it holds in relation to a Data Subject on request;

14.8.8.4 assistance that it requests following any Data Loss Event; and

14.8.8.5 assistance that it requests relating to a consultation with, or request from, the Information Commissioner's Office or any other regulatory authority.

14.8.9 The Processor must maintain full, accurate records and information to show it complies with this clause 14. This requirement does not apply where the Processor employs fewer than 250 staff, unless either the Controller determines that the processing:

14.8.9.1 is not occasional;

14.8.9.2 includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or

14.8.9.3 is likely to result in a risk to the rights and freedoms of Data Subjects.

14.8.10 The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.

14.8.11 Before allowing any Subprocessor to process any Personal Data, the Processor must:

14.8.11.1 notify the Controller in writing of the intended Subprocessor and processing;

14.8.11.2 obtain the written consent of the Controller;

14.8.11.3 enter into a written contract with the Sub-processor so that this clause 14 applies to the Sub-processor; and

14.8.11.4 provide the Controller with any information about the Sub-processor that the Controller reasonably requires.

14.8.12 The Processor remains fully liable for all acts or omissions of any Sub-processor.

14.8.13 The Parties agree to take account of any guidance issued by the Information Commissioner's Office or any other regulatory authority.

14.9 Joint Controllers of Personal Data

In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement paragraphs that are necessary to comply with UK GDPR Article 26 based on the terms set out in Part B Joint Controller Agreement *(Optional)* of Annex –1 Processing Personal Data.

14.10 Independent Controllers of Personal Data

In the event that the Parties are Independent Controllers in respect of Personal Data under the Contract, the terms set out in Part C Independent Controllers *(Optional)* of Annex –1 Processing Personal Data shall apply to this Contract.

15 WHAT YOU MUST KEEP CONFIDENTIAL

15.1 Each Party must:

15.1.1 keep all Confidential Information it receives confidential and secure;

15.1.2 not disclose, use or exploit the disclosing Party's Confidential Information without the disclosing Party's prior written consent, except for the purposes anticipated under the Contract; and

15.1.3 immediately notify the disclosing Party if it suspects unauthorised access, copying, use or disclosure of the Confidential Information.

15.2 In spite of clause 15.1, a Party may disclose Confidential Information which it receives from the disclosing Party in any of the following instances:

15.2.1 where disclosure is required by applicable Law if the recipient Party notifies the disclosing Party of the full circumstances, the affected Confidential Information and extent of the disclosure;

15.2.2 if the recipient Party already had the information without obligation of confidentiality before it was disclosed by the disclosing Party;

15.2.3 if the information was given to it by a third party without obligation of confidentiality;

15.2.4 if the information was in the public domain at the time of the disclosure;

15.2.5 if the information was independently developed without access to the disclosing Party's Confidential Information;

15.2.6 on a confidential basis, to its auditors or for the purposes of regulatory requirements;

15.2.7 on a confidential basis, to its professional advisers on a need-to-know basis; and

15.2.8 to the Serious Fraud Office where the recipient Party has reasonable grounds to believe that the disclosing Party is involved in activity that may be a criminal offence under the Bribery Act 2010.

15.3 The Supplier may disclose Confidential Information on a confidential basis to Supplier Staff on a need-to-know basis to allow the Supplier to meet its obligations under the Contract. The Supplier shall remain responsible at all times for compliance with the confidentiality obligations set out in this Contract by the persons to whom disclosure has been made.

15.4 The Buyer may disclose Confidential Information in any of the following cases:

15.4.1 on a confidential basis to the employees, agents, consultants and contractors of the Buyer;

15.4.2 on a confidential basis to any Crown Body, any successor body to a Crown Body or any company that the Buyer transfers or proposes to transfer all or any part of its business to;

15.4.3 if the Buyer (acting reasonably) considers disclosure necessary or appropriate to carry out its public functions;

15.4.4 where requested by Parliament; and

15.4.5 under clauses 5.8 and 16.

15.5 For the purposes of clauses 15.2 to 15.4 references to disclosure on a confidential basis means disclosure under a confidentiality agreement or arrangement including terms as strict as those required in clause 15.

15.6 Transparency Information and any information which is disclosed under clause 16 is not Confidential Information.

15.7 The Supplier must not make any press announcement or publicise the Contract or any part of it in any way, without the prior written consent of the Buyer and must take all reasonable endeavours to ensure that Supplier Staff do not either.

16 WHEN YOU CAN SHARE INFORMATION

16.1 The Supplier must tell the Buyer within 48 hours if it receives a Request For Information.

16.2 In accordance with a reasonable timetable and in any event within 5 Working Days of a request from the Buyer, at no additional cost, the Supplier must give the Buyer full co-operation and information needed so the Buyer can:

16.2.1 comply with any Request For Information; and

16.2.2 comply with any of its obligations in relation to publishing Transparency Information.

16.3 Any such co-operation and/or information from the Supplier shall be provided at no additional cost.

16.4 To the extent that it is allowed and practical to do so, the Buyer will use reasonable endeavours to notify the Supplier of a Request For Information and may talk to the Supplier to help it decide whether to publish information under clause 16. However, the extent, content and format of the disclosure shall be decided by the Buyer, in its sole discretion.

17 INSURANCE

17.1 The Supplier shall ensure it has adequate insurance cover for this Contract.

18 INVALID PARTS OF THE CONTRACT

18.1 If any provision or part-provision of this Contract 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 Contract. The provisions incorporated into the Contract are the entire agreement between the Parties. The Contract replaces all previous statements, or agreements whether written or oral. No other provisions apply.

19 OTHER PEOPLE'S RIGHTS IN THE CONTRACT

19.1 Subject to clause 19.2, no third parties may use the Contracts (Rights of Third Parties) Act ("**CRTPA**") to enforce any term of the Contract unless stated (referring to CRTPA) in the Contract. This does not affect third party rights and remedies that exist independently from CRTPA.

19.2 Clauses 5.7, 24.4 and 24.5 confer benefits on persons named or identified in such provisions other than the Parties (each such person a **"Third Party Beneficiary"**) and are intended to be enforceable by Third Parties Beneficiaries by virtue of the CRTPA.

20 CIRCUMSTANCES BEYOND YOUR CONTROL

20.1 Any Party affected by a Force Majeure Event is excused from performing its obligations under the Contract while the inability to perform continues, if it both:

20.1.1 provides written notice to the other Party; and

20.1.2 uses all reasonable measures practical to reduce the impact of the Force Majeure Event.

20.2 Any failure or delay by the Supplier to perform its obligations under the Contract that is due to a failure or delay by an agent, Subcontractor and/or Supplier Staff will only be considered a Force Majeure Event if that third party is itself prevented from complying with an obligation to the Supplier due to a Force Majeure Event.

20.3 Either Party can partially or fully terminate the Contract if the provision of the Deliverables is materially affected by a Force Majeure Event which lasts for 90 days continuously and the consequences of termination in clauses 11.5.1.2 to 11.5.1.7 shall apply.

20.4 Where a Party terminates under clause 20.3:

20.4.1 each Party must cover its own losses; and

20.4.2 clauses 11.5.1.2 to 11.5.1.7 apply.

21 RELATIONSHIPS CREATED BY THE CONTRACT

21.1 The Contract does not create a partnership, joint venture or employment relationship. The Supplier must represent themselves accordingly and ensure others do so.

22 GIVING UP CONTRACT RIGHTS

22.1 A partial or full waiver or relaxation of the terms of the Contract is only valid if it is stated to be a waiver in writing to the other Party.

23 TRANSFERRING RESPONSIBILITIES

23.1 The Supplier cannot assign, novate or in any other way dispose of the Contract or any part of it without the Buyer's written consent.

23.2 The Buyer can assign, novate or transfer its Contract or any part of it to any Crown Body, public or private sector body which performs the functions of the Buyer.

23.3 When the Buyer uses its rights under clause 23.2 the Supplier must enter into a novation agreement in the form that the Buyer specifies.

23.4 The Supplier can terminate the Contract novated under clause 23.2 to a private sector body that is experiencing an Insolvency Event.

23.5 The Supplier remains responsible for all acts and omissions of the Supplier Staff as if they were its own.

24 SUPPLY CHAIN

24.1 The Supplier cannot sub-contract the Contract or any part of it without the Buyer's prior written consent. The Supplier shall provide the Buyer with the name of any Subcontractor the Supplier proposes to engage for the purposes of the Contract. The decision of the Buyer to consent or not will not be unreasonably withheld or delayed. If the Buyer does not communicate a decision to the Supplier within 10 Working Days of the request for consent then its consent will be deemed to have been given. The Buyer may reasonably withhold its consent to the appointment of a Subcontractor if it considers that:

24.1.1 the appointment of a proposed Subcontractor may prejudice the provision of the Deliverables or may be contrary to its interests;

24.1.2 the proposed Subcontractor is unreliable and/or has not provided reliable goods and or reasonable services to its other customers; and/or

24.1.3 the proposed Subcontractor employs unfit persons.

24.2 If the Buyer asks the Supplier for details about Subcontractors, the Supplier must provide details of all such Subcontractors at all levels of the supply chain including:

24.2.1 their name;

24.2.2 the scope of their appointment; and

24.2.3 the duration of their appointment.

24.3 The Supplier must exercise due skill and care when it selects and appoints Subcontractors.

24.4 For Sub-Contracts in the Supplier's supply chain which are entered into wholly or substantially for the purpose of performing or contributing to the performance of the whole or any part of this Contract:

i. after the Start Date, the Supplier will ensure that they all contain provisions that; or

ii. on or before the Start Date, the Supplier will take all reasonable endeavours to ensure that they all contain provisions that:

24.4.1 allow the Supplier to terminate the Sub-Contract if the Subcontractor fails to comply with its obligations in respect of environmental, social or employment Law; and

24.4.2 require that all Subcontractors are paid:

24.4.2.1 before the end of the period of 30 days beginning with the day on which an invoice is received by the Supplier or other party in respect of the sum; or

24.4.2.2 if later, the date by which the payment falls due in accordance with the invoice,

subject to the invoice being verified by the party making payment as valid and undisputed;

24.4.3 require the party receiving goods or services under the contract to consider and verify invoices under that contract in a timely fashion and notify the Subcontractor without undue delay if it considers the invoice invalid or it disputes the invoice; and

24.4.4 allow the Buyer to publish the details of the late payment or non-payment if this 30 day limit is exceeded.

24.5 The Supplier must ensure that a term equivalent to Clause 24.4 is included in each Sub-Contract in its supply chain, such that each Subcontractor is obliged to include those terms in any of its own Sub-Contracts in the supply chain for the delivery of this Contract. References to the “Supplier” and “Subcontractor” in clause 24.4 are to be replaced with references to the respective Subcontractors who are parties to the relevant contract.

24.6 At the Buyer's request, the Supplier must terminate any Sub-Contracts in any of the following events:

24.6.1 there is a change of control within the meaning of Section 450 of the Corporation Tax Act 2010 of a Subcontractor which isn't pre-approved by the Buyer in writing;

24.6.2 the acts or omissions of the Subcontractor have caused or materially contributed to a right of termination under clause 11.4;

24.6.3 a Subcontractor or its Affiliates embarrasses or brings into disrepute or diminishes the public trust in the Buyer; and/or

24.6.4 the Subcontractor fails to comply with its obligations in respect of environmental, social or employment Law.

24.7 The Supplier is responsible for all acts and omissions of its Subcontractors and those employed or engaged by them as if they were its own.

25 CHANGING THE CONTRACT

25.1 Either Party can request a variation to the Contract which is only effective if agreed in writing and signed by both Parties. The Buyer is not required to accept a variation request made by the Supplier.

26 HOW TO COMMUNICATE ABOUT THE CONTRACT

26.1 All notices under the Contract shall be in writing and be served by e-mail unless it is not practicable to do so. An e-mail is effective at 9am on the first Working Day after sending unless an error message is received.

26.2 If it is not practicable for a notice to be served by e-mail in accordance with clause 26.1, notices can be served my means of personal delivery or Prepaid, Royal Mail Signed For™ 1st Class or other prepaid, next Working Day service providing proof of delivery. If either of these options are used to serve a notice, such notices are considered effective on the Working Day of delivery as long as they're delivered before 5:00pm on a Working Day. Otherwise, the notice is effective on the next Working Day.

26.3 Notices to the Buyer or Supplier must be sent to their e-mail address (or address, where e-mail is not practicable) in the Order Form.

26.4 This clause does not apply to the service of legal proceedings or any documents in any legal action, arbitration or dispute resolution.

27 DEALING WITH CLAIMS

27.1 If a Beneficiary becomes aware of any Claim, then it must notify the Indemnifier as soon as reasonably practical.

27.2 at the Indemnifier's cost the Beneficiary must:

27.2.1 allow the Indemnifier to conduct all negotiations and proceedings to do with a Claim;

27.2.2 give the Indemnifier reasonable assistance with the Claim if requested; and

27.2.3 not make admissions about the Claim without the prior written consent of the Indemnifier which cannot be unreasonably withheld or delayed.

27.3 The Indemnifier must:

27.3.1 consider and defend the Claim diligently and in a way that does not damage the Beneficiary's reputation; and

27.3.2 not settle or compromise any Claim without the Beneficiary's prior written consent which it must not unreasonably withhold or delay.

28 EQUALITY, DIVERSITY AND HUMAN RIGHTS

28.1 The Supplier must follow all applicable employment and equality Law when they perform their obligations under the Contract, including:

28.1.1 protections against discrimination on the grounds of race, sex, gender reassignment, religion or belief, disability, sexual orientation, pregnancy, maternity, age or otherwise; and

28.1.2 any other requirements and instructions which the Buyer reasonably imposes related to equality Law.

28.2 The Supplier must use all reasonable endeavours, and inform the Buyer of the steps taken, to prevent anything that is considered to be unlawful discrimination by any court or tribunal, or the Equality and Human Rights Commission (or any successor organisation) when working on the Contract.

29 HEALTH AND SAFETY

29.1 The Supplier must perform its obligations meeting the requirements of:

29.1.1 all applicable Law regarding health and safety; and

29.1.2 the Buyer's current health and safety policy while at the Buyer's premises, as provided to the Supplier.

29.2 The Supplier and the Buyer must as soon as possible notify the other of any health and safety incidents or material hazards they're aware of at the Buyer premises that relate to the performance of the Contract.

30 ENVIRONMENT AND SUSTAINABILITY

30.1 In performing its obligations under the Contract, the Supplier shall, to the reasonable satisfaction of the Buyer:

30.1.1 meet, in all material respects, the requirements of all applicable Laws regarding the environment; and

30.1.2 comply with its obligations under the Buyer's current environmental policy, which the Buyer must provide, and make Supplier Staff aware of such policy.

31 TAX

31.1 The Supplier must not breach any tax or social security obligations and must enter into a binding agreement to pay any late contributions due, including where applicable, any interest or any fines. The Buyer cannot terminate the Contract where the Supplier has not paid a minor tax or social security contribution.

31.2 Where the Supplier or any Supplier Staff are liable to be taxed or to pay National Insurance contributions in the UK relating to payment received under the Contract, the Supplier must both:

31.2.1 comply with the Income Tax (Earnings and Pensions) Act 2003, the Social Security Contributions and Benefits Act 1992 and all other statutes and regulations relating to income tax and National Insurance contributions (including IR35); and

31.2.2 indemnify the Buyer against any Income Tax, National Insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made during or after the Term in connection with the provision of the Deliverables by the Supplier or any of the Supplier Staff.

31.3 At any time during the Term, the Buyer may specify information that the Supplier must provide with regard to the Supplier, the Supplier Staff, the Workers, or the Supply Chain Intermediaries and set a deadline for responding, which:

31.3.1 demonstrates that the Supplier, Supplier Staff, Workers, or Supply Chain Intermediaries comply with the legislation specified in Clause 31.2.1, or why those requirements do not apply; and

31.3.2 assists with the Buyer's due diligence, compliance, reporting, or demonstrating its compliance with any of the legislation in Clause 31.2.1.

31.4 The Buyer may supply any information they receive from the Supplier under Clause 31.3 to HMRC for revenue collection and management and for audit purposes.

31.5 The Supplier must inform the Buyer as soon as reasonably practicable if there any Workers or Supplier Staff providing services to the Buyer who are contracting, begin contracting, or stop contracting via an intermediary which meets one of conditions A-C set out in section 61N of the Income Tax (Earnings and Pensions) Act 2003 and/or Regulation 14 of the Social Security Contributions (Intermediaries) Regulations 2000.

31.6 If any of the Supplier Staff are Workers who receive payment relating to the Deliverables, then the Supplier must ensure that its contract with the Worker contains requirements that:

31.6.1 the Buyer may, at any time during the term of the Contract, request that the Worker provides information which demonstrates they comply with clause 31.2, or why those requirements do not apply, the Buyer can specify the information the Worker must provide and the deadline for responding;

31.6.2 the Worker's contract may be terminated at the Buyer's request if the Worker fails to provide the information requested by the Buyer within the time specified by the Buyer;

31.6.3 the Worker's contract may be terminated at the Buyer's request if the Worker provides information which the Buyer considers isn't good enough to demonstrate how it complies with clause 31.2 or confirms that the Worker is not complying with those requirements; and

31.6.4 the Buyer may supply any information they receive from the Worker to HMRC for revenue collection and management.

32 CONFLICT OF INTEREST

32.1 The Supplier must take action to ensure that neither the Supplier nor the Supplier Staff are placed in the position of an actual or potential Conflict of Interest.

32.2 The Supplier must promptly notify and provide details to the Buyer if an actual, perceived or potential Conflict of Interest happens or is expected to happen.

32.3 The Buyer will consider whether there are any reasonable steps that can be put in place to mitigate an actual, perceived or potential Conflict of Interest. If, in the reasonable opinion of the Buyer, such steps do not or will not resolve an actual or potential Conflict of Interest, the Buyer may terminate the Contract immediately by giving notice in writing to the Supplier where there is or may be an actual or potential Conflict of Interest and, subject to clause 32.4, where the reason for the unresolvable actual or potential Conflict of Interest is in the reasonable opinion of the Buyer

32.3.1 outside of the control of the Supplier, clauses 11.5.1.2 to 11.5.1.7 shall apply

32.3.2 within the control of the Supplier, the whole of clause 11.5.1 shall apply.

32.4 Where the Supplier has failed to notify the Buyer about an actual or potential Conflict of Interest and the Buyer terminates under clause 32.3, the whole of clause 11.5.1 shall apply.

33 REPORTING A BREACH OF THE CONTRACT

33.1 As soon as it is aware of it the Supplier and Supplier Staff must report to the Buyer any actual or suspected breach of Law, clause 13.1, or clauses 27 to 32.

33.2 The Supplier must not retaliate against any of the Supplier Staff who in good faith reports a breach listed in clause 33.1 to the Buyer or a Prescribed Person.

34 FURTHER ASSURANCES

34.1 Each Party will, at the request and cost of the other Party, do all things which may be reasonably necessary to give effect to the meaning of this Contract.

35 RESOLVING DISPUTES

35.1 If there is a dispute between the Parties, their senior representatives who have authority to settle the dispute will, within 28 days of a written request from the other Party, meet in good faith to resolve the dispute by commercial negotiation.

35.2 If the dispute is not resolved at that meeting, the Parties can attempt to settle it by mediation using the Centre for Effective Dispute Resolution ("**CEDR**") Model Mediation Procedure current at the time of the dispute. If the Parties cannot agree on a mediator, the mediator will be nominated by CEDR. If either Party does not wish to use, or continue to use mediation, or mediation does not resolve the dispute, the dispute must be resolved using clauses 35.3 to 35.5.

35.3 Unless the Buyer refers the dispute to arbitration using clause 35.4, the Parties irrevocably agree that the courts of England and Wales have exclusive jurisdiction.

35.4 The Supplier agrees that the Buyer has the exclusive right to refer any dispute to be finally resolved by arbitration under the London Court of International Arbitration Rules current at the time of the dispute. There will be only one arbitrator. The seat or legal place of the arbitration will be London and the proceedings will be in English.

35.5 The Buyer has the right to refer a dispute to arbitration even if the Supplier has started or has attempted to start court proceedings under clause 35.3, unless the Buyer has agreed to the court proceedings or participated in them. Even if court proceedings have started, the Parties must do everything necessary to ensure that the court proceedings are stayed in favour of any arbitration proceedings if they are started under clause 35.4.

35.6 The Supplier cannot suspend the performance of the Contract during any dispute.

36 WHICH LAW APPLIES

36.1 This Contract and any issues or disputes arising out of, or connected to it, are governed by English law.

V. Annex –1 Processing Personal Data

[Guidance: Part A of this Annex is mandatory. The Buyer will be the Controller, and the Supplier the Processor in the vast majority of cases. If the Buyer believes another data processing scenario applies, such as the Parties being Joint or Independent Controllers, the Buyer must speak to its data protection team or DPO. Making the Supplier a Controller over Buyer information can create risks for the Buyer, and the Buyer must make sure it understands the consequences of this. If the Buyer needs further guidance around how to complete this Annex, see Schedule 20 of the Mid-Tier Contract and/or speak to your DPO]

Part A Authorised Processing Template

This Annex 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 Annex shall be with the Controller at its absolute discretion.

The contact details of the Controller's Data Protection Officer are: [**Insert** Contact details]

The contact details of the Processor's Data Protection Officer are: [**Insert** Contact details]

The Processor shall comply with any further written instructions with respect to processing by the Controller.

Any such further instructions shall be incorporated into this Annex.

Description of authorised processing	Details
Identity of Controller and Processor / Independent Controllers / Joint Controllers for each category of Personal Data	***[Guidance: This is where the Buyer identifies the roles of the Parties for processing personal data. If the Parties are Independent Controllers or Joint Controllers the Buyer will use Part B or Part C of this Annex as applicable, see Annex 1 of Schedule 20 of the Mid-Tier for further details]***
Subject matter of the processing	
Duration of the processing	
Nature and purposes of the processing	
Type of Personal Data being processed	
Categories of Data Subject	
Plan for return and destruction of the data once the processing is complete UNLESS requirement under law to preserve that type of data	
Locations at which the Supplier and/or its Subcontractors process Personal Data under this Contract and International transfers and legal gateway	

Protective Measures that the Supplier and, where applicable, its Subcontractors 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 Annex 6 *(Security Management)*, if used)	[Any Protective Measures must be in accordance with any Security Requirements.]

Part B Joint Controller Agreement *(Optional)*

[Guidance: Not mandatory. Insert the following clauses if the Parties are Joint Controllers of any Personal Data/delete if not using and otherwise mark as "Not Used". Even if deleting the text, keep the heading above so as to retain the cross-reference in the Conditions. The Buyer will be the Controller, and the Supplier the Processor in the vast majority of cases. If the Buyer believes another data processing scenario applies, such as the Parties being Joint or Independent Controllers, the Buyer must speak to its data protection team or DPO]

1 JOINT CONTROLLER STATUS AND ALLOCATION OF RESPONSIBILITIES

1.1 With respect to Personal Data for which the Parties are Joint Controllers, the Parties envisage that they shall each be a Controller in respect of that Personal Data in accordance with the terms of this Part B Joint Controller Agreement *(Optional)* of Annex –1 Processing Personal Data in replacement of clauses 14.8.1 to 14.8.13 of the Conditions of this Contract. Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their processing of such Personal Data as Controllers.

1.2 The Parties agree that the [Supplier/Buyer]:

1.2.1 is the exclusive point of contact for Data Subjects and is responsible for using best endeavours to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;

1.2.2 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;

1.2.3 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;

1.2.4 is responsible for obtaining the informed consent of Data Subjects, in accordance with the UK GDPR, for processing in connection with the Deliverables where consent is the relevant legal basis for that processing; and

1.2.5 shall make available to Data Subjects the essence of this Part B Joint Controller Agreement *(Optional)* of Annex –1 Processing Personal Data (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/Buyer's] privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of Paragraph 1.2 of this Part B Joint Controller Agreement *(Optional)* of Annex –1 Processing Personal Data, 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 Controller.

2 UNDERTAKINGS OF BOTH PARTIES

2.1 The Supplier and the Buyer each undertake that they shall:

2.1.1 report to the other Party every [x] months on:

2.1.1.1 the volume of Data Subject Access Requests (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);

2.1.1.2 the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;

2.1.1.3 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;

2.1.1.4 any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and

2.1.1.5 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;

2.1.2 notify each other immediately if it receives any request, complaint or communication made as referred to in Paragraphs 2.1.1.1 to 2.1.1.5 of this Part B Joint Controller Agreement *(Optional)* of Annex –1 Processing Personal Data;

2.1.3 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 2.1.1.3 to 2.1.1.5 of this Part B Joint Controller Agreement *(Optional)* of Annex –1 Processing Personal Data; to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;

2.1.4 not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Deliverables and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the 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, the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this of this of this Part B Joint Controller Agreement *(Optional)* of Annex –1 Processing Personal Data;

2.1.5 request from the Data Subject only the minimum information necessary to provide the Deliverables and treat such extracted information as Confidential Information;

2.1.6 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;

2.1.7 use best endeavours to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that Processor Personnel:

2.1.7.1 are aware of and comply with their duties under this of this Part B Joint Controller Agreement *(Optional)* of Annex –1 Processing Personal Data; and those in respect of Confidential Information;

2.1.7.2 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;

2.1.7.3 have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;

2.1.8 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;

2.1.9 ensure that it notifies the other Party as soon as it becomes aware of a Data Loss Event; and

2.1.10 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:

2.1.10.1 the transfer is 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 Subcontractors and/or Subprocessors), the Supplier (and/or the applicable Subcontractor and/or Subprocessor) must be self-certified and continue to be self-certified on the US Data Privacy Framework;

(b) the Supplier shall notify the Buyer immediately if there are any, or there are reasonable grounds to believe there may be any, changes in respect of their and/or their Subcontractor's or Subprocessor'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 2.1.10.1; and

(c) in the event that the Supplier (and/or the applicable Subcontractor or Subprocessor):

i. 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 2.1.10.1;

ii. 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 2.1.10.1; and/or

iii. fails to notify the Buyer of any changes to its certification status in accordance with Paragraph 2.1.10.1(b) above,

the Buyer shall have the right to terminate this Contract with immediate effect; or

2.1.10.2 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 the transfer is in accordance with Article 46 of the EU GDPR (where applicable)) as agreed with the non-transferring Party which could include the relevant parties entering into:

(a) where the transfer is subject to the UK GDPR:

i. The UK International Data Transfer Agreement (the "IDTA"), as published by the Information Commissioner's office under section 119A(1) of the DPA 2018 from time to time; or

ii. 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 ("EU SCCs"), together with the UK International Data Transfer Agreement Addendum to the EU SCCs (the "Addendum") as published by the Information Commissioner's Office from time to time and/or;

(b) where the transfer is subject to the EU GDPR, the EU SCCs,

as well as any additional measures determined by the non-transferring Party being implemented by the importing Party;

2.1.10.3 the Data Subject has enforceable rights and effective legal remedies;

2.1.10.4 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

2.1.10.5 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.

2.1.11 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.

3 DATA PROTECTION BREACH

3.1 Without prejudice to Paragraph 3.2 of this Part B Joint Controller Agreement *(Optional)* of Annex – 1 Processing Personal Data, 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:

3.1.1 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;

3.1.2 all reasonable assistance, including:

3.1.2.1 co-operation with the other Party, the Information Commissioner and any other regulatory body investigating the Data Loss Event and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;

3.1.2.2 co-operation with the other Party including using such best endeavours as are directed by the Buyer to assist in the investigation, mitigation and remediation of a Data Loss Event;

3.1.2.3 co-ordination with the other Party regarding the management of public relations and public statements relating to the Data Loss Event; and/or

3.1.2.4 providing the other Party and to the extent instructed by the other Party to do so, the Information Commissioner and/or any other regulatory body investigating the Data Loss Event, with complete information relating to the Data Loss Event, including the information set out in Paragraph 3.2 of this Part B Joint Controller Agreement *(Optional)* of Annex –1 Processing Personal Data;.

3.2 Each Party shall use best endeavours 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:

3.2.1 the nature of the Data Loss Event;

3.2.2 the nature of Personal Data affected;

3.2.3 the categories and number of Data Subjects concerned;

3.2.4 the name and contact details of the Party's Data Protection Officer or other relevant contact from whom more information may be obtained;

3.2.5 measures taken or proposed to be taken to address the Data Loss Event; and

3.2.6 a description of the likely consequences of the Data Loss Event.

4 AUDIT

4.1 The Supplier shall permit:

4.1.1 the Buyer, or a third-party auditor acting under the Buyer's direction, to conduct, at the Buyer'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 of this Part B Joint Controller Agreement *(Optional)* of Annex –1 Processing Personal Data; and the Data Protection Legislation; and/or

4.1.2 the Buyer, or a third-party auditor acting under the Buyer'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 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 Deliverables.

4.2 The Buyer may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Paragraph 4.1 of this Part B Joint Controller Agreement *(Optional)* of Annex –1 Processing Personal Data in lieu of conducting such an audit, assessment or inspection.

5 IMPACT ASSESSMENTS

5.1 The Parties shall:

5.1.1 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

5.1.2 maintain full and complete records of all processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 UK GDPR.

6 ICO GUIDANCE

6.1 The Parties agree to take account of any non-mandatory guidance issued by the Information Commissioner or any other regulatory authority. The Buyer may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant Crown Body.

7 LIABILITIES FOR DATA PROTECTION BREACH

[Guidance: This Paragraph represents a risk share, the Buyer 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]

7.1 If financial penalties are imposed by the Information Commissioner and/or any other regulatory body on either the Buyer or the Supplier for a Data Loss Event ("**Financial Penalties**") then the following shall occur:

7.1.1 if in the view of the Information Commissioner and/or any other regulatory body, the Buyer is responsible for the Data Loss Event, in that it is caused as a result of the actions or inaction of the Buyer, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Buyer, then the Buyer shall be responsible for the payment of such Financial Penalties. In this case, the Buyer 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 Loss Event. The Supplier shall provide to the Buyer 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 Loss Event;

7.1.2 if in the view of the Information Commissioner and/or any other regulatory body, the Supplier is responsible for the Data Loss Event, in that it is not a Data Loss Event that the Buyer is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Buyer and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Data Loss Event; or

7.1.3 if no view as to responsibility is expressed by the Information Commissioner and/or any other regulatory body, then the Buyer and the Supplier shall work together to investigate the relevant Data Loss Event 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 clause 35 of the Conditions (Resolving disputes).

7.2 If either the Buyer 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 Data Loss Event. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Data Loss Event (the "**Claim Losses**"):

7.3.1 if the Buyer is responsible for the relevant Data Loss Event, then the Buyer shall be responsible for the Claim Losses;

7.3.2 if the Supplier is responsible for the relevant Data Loss Event, then the Supplier shall be responsible for the Claim Losses: and

7.3.3 if responsibility for the relevant Data Loss Event is unclear, then the Buyer and the Supplier shall be responsible for the Claim Losses equally.

7.4 Nothing in either Paragraph 7.2 or Paragraph 7.3 of this Part B Joint Controller Agreement *(Optional)* of Annex –1 Processing Personal Data shall preclude the Buyer 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 Data Loss Event and the legal and financial obligations of the Buyer.

8 TERMINATION

8.1 If the Supplier is in Material Breach under any of its obligations under this of this Part B Joint Controller Agreement *(Optional)* of Annex –1 Processing Personal Data;, the Buyer shall be entitled to terminate the Contract by issuing a termination notice to the Supplier in accordance with clause 11 of the Conditions (Ending the contract).

9 SUB-PROCESSING

9.1 In respect of any processing of Personal Data performed by a third party on behalf of a Party, that Party shall:

9.1.1 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 the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and

9.1.2 ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

10 DATA RETENTION

10.1 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 the Party for statutory compliance purposes or as otherwise required by the Contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy.

Part C Independent Controllers *(Optional)*

[Guidance: Not mandatory. Insert the following clauses if the Parties are Independent Controllers of any Personal Data/delete if not using and otherwise mark as "Not Used". Even if deleting the text, keep the heading above so as to retain the cross-reference in the Conditions. The Buyer will be the Controller, and the Supplier the Processor in the vast majority of cases. If the Buyer believes another data processing scenario applies, such as the Parties being Joint or Independent Controllers, the Buyer must speak to its data protection team or DPO]

1 INDEPENDENT CONTROLLER PROVISIONS

1.1 With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their processing of such Personal Data as Controller.

1.2 Each Party shall process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.

1.3 Where a Party has provided Personal Data to the other Party in accordance with Paragraph 1.1 of this Part C Independent Controllers *(Optional)* of Annex –1 Processing Personal Data above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.

1.4 The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the processing of Personal Data for the purposes of the Contract.

1.5 The Parties shall only provide Personal Data to each other:

1.5.1 to the extent necessary to perform their respective obligations under the Contract;

1.5.2 in compliance with the Data Protection Legislation (including by ensuring all required fair processing information has been given to affected Data Subjects);

1.5.3 where the provision of Personal Data from one Party to another involves transfer of such data to outside the UK and/or the EEA, if the prior written consent of the non-transferring Party has been obtained and the following conditions are fulfilled:

1.5.3.1 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 Subcontractors and/or Subprocessors), the Supplier (and/or the applicable Subcontractor and/or Subprocessor) must be self-certified and continue to be self-certified on the US Data Privacy Framework;

(b) the Supplier shall notify the Buyer immediately if there are any, or there are reasonable grounds to believe there may be any, changes in respect of their and/or their Subcontractor's or Subprocessor'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 1.5.3.1; and

(c) in the event that the Supplier (and/or the applicable Subcontractor or Subprocessor):

i. 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 1.5.3.1;

ii. 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 1.5.3.1; and/or

iii. fails to notify the Buyer of any changes to its certification status in accordance with Paragraph 1.5.3.1(b) above,

the Buyer shall have the right to terminate this Contract with immediate effect; or

1.5.3.2 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 determined by the non-transferring Party which could include the parties entering into:

(a) where the transfer is subject to UK GDPR:

i. 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

ii. 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 (the "**EU SCCs**"), together with the UK International Data Transfer Agreement Addendum to the EU SCCs (the "**Addendum**") as published by the Information Commissioner's Office from time to time; and/or

(b) where the transfer is subject to EU GDPR, the EU SCCs;

as well as any additional measures determined by the non-transferring Party being implemented by the importing party;

1.5.3.3 the Data Subject has enforceable rights and effective legal remedies;

1.5.3.4 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

1.5.3.5 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

1.5.4 where it has recorded it in Part A Authorised Processing Template of Annex –1 Processing Personal Data.

1.6 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.

1.7 A Party processing Personal Data for the purposes of the Contract shall maintain a record of its processing activities in accordance with Article 30 UK GDPR and shall make the record available to the other Party upon reasonable request.

1.8 Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract ("**Request Recipient**"):

1.8.1 the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or

1.8.2 where the request or correspondence is directed to the other Party and/or relates to that other Party's processing of the Personal Data, the Request Recipient will:

1.8.2.1 promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and

1.8.2.2 provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.

1.9 Each Party shall promptly notify the other Party upon it becoming aware of any Data Loss Event relating to Personal Data provided by the other Party pursuant to the Contract and shall:

1.9.1 do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Data Loss Event;

1.9.2 implement any measures necessary to restore the security of any compromised Personal Data;

1.9.3 work with the other Party to make any required notifications to the Information Commissioner's office or any other regulatory authority and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and

1.9.4 not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.

1.10 Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Part A Authorised Processing Template of Annex –1 Processing Personal Data.

1.11 Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Part A Authorised Processing Template of Annex –1 Processing Personal Data.

1.12 Notwithstanding the general application of clauses 14.8.1 to 14.8.13 of the Conditions to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with Paragraphs 1.1 to 1.12 of this Part C Independent Controllers *(Optional)* of Annex –1 Processing Personal Data

VI. [Annex –2 Specification] (Optional)

[**Insert** the specification here if using/delete if not using or otherwise mark as "Not Used"]

VII. [Annex –3 Charges] (Optional)

[**Insert** the charges document here if using/delete if not using or otherwise mark as "Not Used"]

VIII. [Annex 4 – Supplier Tender] (Optional)

[**Insert** the tender document here if using/delete if not using or otherwise mark as "Not Used"]

[Guidance: Please note that some parts of the tender documentation may not be appropriate for inclusion (e.g. customer testimonials), and it may be necessary to include any clarifications/updates so that the tender reflects the agreed position.]

IX. [Annex 5 – Optional IPR Clauses] (Optional)

[***Delete if not using and otherwise mark as "Not Used". Even if deleting the text, keep the heading above so as to retain the cross-reference in the Order Form***]

[Guidance: The clauses in this [Annex 5 – Optional IPR Clauses] (Optional) on Intellectual Property Rights ("IPRs") can be included in place of the default clause 10 of the Conditions depending on how the Buyer needs to arrange ownership and licencing of all New IPR created for or pursuant to the Contract. There are a further 2 suggested options available.

Default Option (Option 1) (clause 10 of the Conditions): Buyer owns all New IPR with non-exclusive Supplier rights to all New IPR.

The new options are:

Part A of [Annex 5 – Optional IPR Clauses] (Optional) (Option 2): Buyer ownership of all New IPR with limited Supplier rights to all New IPR in order to deliver the Contract; and

Part B of [Annex 5 – Optional IPR Clauses] (Optional) (Option 3): Supplier ownership of all New IPR with Buyer rights for the current contract and broader public sector functions.

Option 1 should be considered for use in situations where the Buyer should retain ownership of any New IPR but where the Supplier should be able to use any New IPR developed. In this situation, the Buyer will not look to publish the New IPR under Open Licence.

Option 2 should be considered for use where the Buyer should retain ownership of any New IPR and ensure that the Supplier cannot use it outside of Contract delivery.

Option 3 should be considered for use where (a) there is no clear benefit in the Buyer owning the New IPR, or (b) where any New IPR created cannot easily be separated from the Supplier's Existing IPR (e.g. Software As A Service ("SAAS")) and should be used where the licence to the Buyer for the IPR in question should extend to cover other government contracts and services, which may include contracts and services not yet awarded, and broader public sector functions.

When publishing as open source, Buyers should be mindful that the terms of any input licence (that is the open source licence for any open source intellectual property which has been used to create the New IPR) aligns with the 'output licence' (that is, the licence under which the Buyer will publish the New IPR as open source).]

Part A Buyer ownership with limited Supplier rights to exploit New IPR for the purposes of the current Contract

[Guidance: Not mandatory. See above. Check paragraph numbers are correct, including cross-references]

1 INTELLECTUAL PROPERTY RIGHTS ("IPRS")

1.1 Each Party keeps ownership of its own Existing IPRs. The Supplier gives the Buyer a non-exclusive, perpetual, royalty-free, irrevocable, transferable, sub-licensable worldwide licence to use, copy and adapt the Supplier's Existing IPR to enable the Buyer and its sub-licensees to both:

1.1.1 receive and use the Deliverables; and

1.1.2 use the New IPR.

The termination or expiry of the Contract does not terminate any licence granted under this clause 1.

1.2 Any New IPR created under the Contract is owned by the Buyer. The Buyer gives the Supplier a royalty-free, non-exclusive, non-transferable licence to use, copy and adapt any Existing IPRs and the New IPR for the purpose of fulfilling its obligations during the Term. This licence is sub-licensable to a Subcontractor for the purpose of enabling the Supplier to fulfil its obligations under the Contract, and in that case the Subcontractor must enter into a confidentiality undertaking with the Supplier on the same terms as set out in clause 15 (What you must keep confidential).

1.3 Unless otherwise agreed in writing, the Supplier and the Buyer will record any New IPR and keep this record updated throughout the Term.

1.4 Where a Party acquires ownership of intellectual property rights incorrectly under this Contract it must do everything reasonably necessary to complete a transfer assigning them in writing to the other Party on request and at its own cost.

1.5 Neither Party has the right to use the other Party's intellectual property rights, including any use of the other Party's names, logos or trademarks, except as provided in clause 1 or otherwise agreed in writing.

1.6 If any claim is made against the Buyer for actual or alleged infringement of a third party's intellectual property arising out of, or in connection with, the supply or use of the Deliverables (an "**IPR Claim**"), then the Supplier indemnifies the Buyer against all losses, damages, costs or expenses (including professional fees and fines) incurred as a result of the IPR Claim.

1.7 If an IPR Claim is made or anticipated the Supplier must at its own option and expense, either:

1.7.1 obtain for the Buyer the rights in clause 1.1 without infringing any third party intellectual property rights; and

1.7.2 replace or modify the relevant item with substitutes that don't infringe intellectual property rights without adversely affecting the functionality or performance of the Deliverables.

1.8 If the Supplier is not able to resolve the IPR Claim to the Buyer's reasonable satisfaction within a reasonable time, the Buyer may give written notice that it terminates the Contract from the date set out in the notice, or where no date is given in the notice, the date of the notice. On termination, the consequences of termination in clause 11.5.1 shall apply.

1.9 The Supplier shall not use in the Delivery of the Deliverables any Third Party IPR unless:

1.9.1 the Buyer gives its approval to do so; and

1.9.2 one of the following conditions applies:

1.9.2.1 the owner or an authorised licensor of the relevant Third Party IPR has granted the Buyer a direct licence that provides the Buyer with the rights in clause 1.1; or

1.9.2.2 if the Supplier cannot, after commercially reasonable endeavours, obtain for the Buyer a direct licence to the Third Party IPR as set out in clause 1.9.2.1:

(a) the Supplier provides the Buyer with details of the licence terms it can obtain and the identity of those licensors;

(b) the Buyer agrees to those licence terms; and

(c) the owner or authorised licensor of the Third Party IPR grants a direct licence to the Buyer on those terms; or

1.9.2.3 the Buyer approves in writing, with reference to the acts authorised and the specific intellectual property rights involved.

1.10 In spite of any other provisions of the Contract and for the avoidance of doubt, award of this Contract by the Buyer and the ordering of any Deliverable under it, does not constitute an authorisation by the Crown under Sections 55 and 56 of the Patents Act 1977, Section 12 of the Registered Designs Act 1949 or Sections 240 – 243 of the Copyright, Designs and Patents Act 1988.

1.11 Subject to clause 1.10, the Supplier agrees that the Buyer may at its sole discretion publish under Open Licence all or part of the New IPR Items and the Supplier warrants that the New IPR Items are suitable for release under Open Licence and that the publication of the New IPR Items under Open Licence will not infringe the rights of any third party and will not harm any Third Party or the Buyer.

1.12 The Supplier will supply any or all New IPR Items in a format suitable for publication under Open Licence ("**Open Licence Publication Material**") within 30 days of written request from the Buyer ("**Buyer Open Licence Request**"). Where any Supplier Existing IPR is included in the Open Licence Publication Material, this will become Open Licence material.

1.13 The Supplier may within 15 days of a Buyer Open Licence Request under clause 1.12, request in writing that the Buyer excludes all or part of:

1.13.1 the New IPR; or

1.13.2 Supplier Existing IPR or Third Party IPR that would otherwise be included in the Open Licence Publication Material supplied to the Buyer pursuant to clause 1.12

from Open Licence publication.

1.14 Any decision to approve any such request from the Supplier pursuant to clause 1.13 shall be at the Buyer's sole discretion, not to be unreasonably withheld, delayed or conditioned.

1.15 Subject to clause 12, the Buyer will not be liable in the event that any Supplier Existing IPR or Third Party IPR is included in the Open Licence Publication Material published by the Buyer.

Part B Supplier ownership of New IPR with Buyer rights for the current Contract and broader public sector functions

[Guidance: Not mandatory. See above. Check paragraph numbers are correct, including cross-references]

1 INTELLECTUAL PROPERTY RIGHTS ("IPRS")

1.1 Each Party keeps ownership of its own Existing IPRs. Any New IPR created under the Contract is owned by the Supplier. The Supplier gives the Buyer a non-exclusive, perpetual, royalty-free, irrevocable, transferable, sub-licensable worldwide licence to use, copy and adapt the Supplier's Existing IPR and the New IPR to enable the Buyer and its sub-licensees to receive and use the Deliverables and the New IPR for any purpose relating to the exercise of the Buyer's (or, if the Buyer is a Public Sector Body, any other Public Sector Body's) business or function. For the purposes of this clause "**Public Sector Body**" means a formally established organisation that is (at least in part) publicly funded to deliver a public or government service.

1.2 The termination or expiry of the Contract does not terminate any licence granted under this clause 1.

1.3 The Buyer gives the Supplier a royalty-free, non-exclusive, non-transferable licence to use, copy, and adapt any Existing IPRs for the purpose of fulfilling its obligations during the Term and commercially exploiting the New IPR developed under the Contract. This licence is sub-licensable to a Subcontractor for the purpose of enabling the Supplier to fulfil its obligations under the Contract, and in that case the Subcontractor must enter into a confidentiality undertaking with the Supplier on the same terms as set out in clause 15 (What you must keep confidential).

1.4 Unless otherwise agreed in writing, the Supplier and the Buyer will record any New IPR and keep this record updated throughout the Term.

1.5 Where a Party acquires ownership of intellectual property rights incorrectly under this Contract it must do everything reasonably necessary to complete a transfer assigning them in writing to the other Party on request and at its own cost.

1.6 Neither Party has the right to use the other Party's intellectual property rights, including any use of the other Party's names, logos or trademarks, except as provided in this clause 1 or otherwise agreed in writing.

1.7 If any claim is made against the Buyer for actual or alleged infringement of a third party's intellectual property arising out of, or in connection with, the supply or use of the Deliverables (an "**IPR Claim**"), then the Supplier indemnifies the Buyer against all losses, damages, costs or expenses (including professional fees and fines) incurred as a result of the IPR Claim.

1.8 If an IPR Claim is made or anticipated, the Supplier must at its own option and expense, either:

1.8.1 obtain for the Buyer the rights in clause 1.1 without infringing any third party intellectual property rights; and

1.8.2 replace or modify the relevant item with substitutes that don't infringe intellectual property rights without adversely affecting the functionality or performance of the Deliverables.

1.9 If the Supplier is not able to resolve the IPR Claim to the Buyer's reasonable satisfaction within a reasonable time, the Buyer may give written notice that it terminates the Contract from the date set out in the notice, or where no date is given in the notice, the date of the notice. On termination, the consequences of termination in clause 11.5.1 shall apply.

1.10 The Supplier shall not use in the Delivery of the Deliverables any Third Party IPR unless:

1.10.1 the Buyer gives its approval to do so; and

1.10.2 one of the following conditions applies:

1.10.2.1 the owner or an authorised licensor of the relevant Third Party IPR has granted the Buyer a direct licence that provides the Buyer with the rights in clause 1.1; or

1.10.2.2 if the Supplier cannot, after commercially reasonable endeavours, obtain for the Buyer a direct licence to the Third Party IPR as set out in clause 1.10.2.1:

(a) the Supplier provides the Buyer with details of the licence terms it can obtain and the identity of those licensors;

(b) the Buyer agrees to those licence terms; and

(c) the owner or authorised licensor of the Third Party IPR grants a direct licence to the Buyer on those terms; or

1.10.2.3 the Buyer approves in writing, with reference to the acts authorised and the specific intellectual property rights involved.

1.11 In spite of any other provisions of the Contract and for the avoidance of doubt, award of this Contract by the Buyer and the ordering of any Deliverable under it, does not constitute an authorisation by the Crown under Sections 55 and 56 of the Patents Act 1977, Section 12 of the Registered Designs Act 1949 or Sections 240 – 243 of the Copyright, Designs and Patents Act 1988.

X. [Annex 6 – Security Management] (Optional)

[Guidance: See https://www.security.gov.uk/policy-and-guidance/contracting-securely/ for further guidance. If the Contract relates to a particularly high-risk security project, or if the Buyer is buying consultancy or development services, the Buyer may want to consider adapting one of the other Mid-Tier Contract Security Schedules (Schedule 16) for inclusion in this Annex 6]

1 SUPPLIER OBLIGATIONS

Core requirements

1.1 The Supplier must comply with the core requirements set out in Paragraphs 3 to 9.

1.2 Where the Buyer 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:

Certifications (see Paragraph 4)		
The Supplier must have the following Certifications (or equivalent):	ISO/IEC 27001:2022 by a UKAS-recognised Certification Body	☐
	Cyber Essentials Plus	☐
	Cyber Essentials	☐
	No certification required	☐
Sub-contractors that Handle Government Data must have the following Certifications (or equivalent):	ISO/IEC 27001:2022 by a UKAS-recognised Certification Body	☐
	Cyber Essentials Plus	☐
	Cyber Essentials	☐
	No certification required	☐
Locations (see Paragraph 5)		
The Supplier and Sub-contractors may store, access or Handle Government Data in:	the United Kingdom only	☐
	a location permitted by and in accordance with any regulations for the time being in force made under 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State)	☐
	anywhere in the world not prohibited by the Buyer	☐
Staff vetting (see Paragraph 6)		
The Buyer requires a staff vetting procedure other than BPSS		☐
Where an alternative staff vetting procedure is required, the procedure is: [**Set out required staff vetting procedure (other than BPSS)**]		

Optional requirements

1.3 Where the Buyer has selected an option in the table below, the Supplier must comply with the requirements of the corresponding Paragraph. Where the Buyer has not selected an option, the corresponding requirement does not apply.

Security Management Plan (see Paragraph 1 of Part B *(Additional Requirements)*)	
The Supplier must provide the Buyer with a Security Management Plan detailing how the requirements for the options selected in this table have been met.	☐
Buyer Security Policies (see Paragraph 2 of Part B *(Additional Requirements)*)	
The Buyer requires the Supplier to comply with the following policies relating to security management: • [**List Buyer security policies with which the Supplier and Subcontractors must comply**].	☐
Security testing (see Paragraph 3 of Part B *(Additional Requirements)*)	
The Supplier must undertake security testing at least once every Contract Year and remediate any vulnerabilities, where it is technically feasible to do so	☐
Cloud Security Principles (see Paragraph 4 of Part B *(Additional Requirements)*)	
The Supplier must assess the Supplier System against the Cloud Security Principles	☐
Record keeping (see Paragraph 5 of Part B *(Additional Requirements)*)	
The Supplier must keep records relating to Sub-contractors, Sites, Third-Party Tools and third parties	☐
Encryption (see Paragraph 6 of Part B *(Additional Requirements)*)	
The Supplier must encrypt Government Data while at rest or in transit	☐
Protective Monitoring System (see Paragraph 7 of Part B *(Additional Requirements)*)	
The Supplier must implement an effective Protective Monitoring System	☐
Patching (see Paragraph 8 of Part B *(Additional Requirements)*)	
The Supplier must patch vulnerabilities in the Supplier System promptly	☐
Malware protection (see Paragraph 9 of Part B *(Additional Requirements)*)	
The Supplier must use appropriate Anti-virus Software	☐
End-User Devices (see Paragraph 10 of Part B *(Additional Requirements)*)	
The Supplier must manage End-User Devices appropriately	☐
Vulnerability scanning (see Paragraph 11 of Part B *(Additional Requirements)*)	
The Supplier must scan the Supplier System monthly for unpatched vulnerabilities	☐

Access control (see Paragraph 12 of Part B *(Additional Requirements)*)	
The Supplier must implement effective access control measures for those accessing Government Data and for Privileged Users	☐
Remote Working (see Paragraph 13 of Part B *(Additional Requirements)*)	
The Supplier may allow Supplier Staff to undertake Remote Working once an approved Remote Working Policy is in place	☐
Backup and recovery of Government Data (see Paragraph 14 of Part B *(Additional Requirements)*)	
The Supplier must have in place systems for the backup and recovery of Government Data	☐
Return and deletion of Government Data (see Paragraph 15 of Part B *(Additional Requirements)*)	
The Supplier must return or delete Government Data when requested by the Buyer	☐
Physical security (see Paragraph 16 of Part B *(Additional Requirements)*)	
The Supplier must store Government Data in physically secure locations	☐
Security breaches (see Paragraph 17 of Part B *(Additional Requirements)*)	
The Supplier must report any Breach of Security to the Buyer promptly	☐

2 DEFINITIONS

[Guidance: The defined term 'Government Data' used within this Annex can be found within Clause 1 (Definitions used in the Contract)]

"Anti-virus Software"	software that: (a) protects the Supplier System from the possible introduction of Malicious Software; (b) scans for and identifies possible Malicious Software in the Supplier System; (c) if Malicious Software is detected in the Supplier System, so far as possible: (i) prevents the harmful effects of the Malicious Software; and (ii) removes the Malicious Software from the Supplier System;
"BPSS"	the employment controls applied to any individual member of the Supplier Staff 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;
"Breach of Security"	the occurrence of:

	(a) any unauthorised access to or use of the Services, the Sites, the Supplier System and/or the Government Data; (b) the loss (physical or otherwise), corruption and/or unauthorised disclosure of any Government Data, including copies of such Government Data; and/or (c) any part of the Supplier System ceasing to be compliant with the required Certifications; (d) the installation of Malicious Software in the Supplier System: (e) any loss of operational efficiency or failure to operate to specification as the result of the installation or operation of Malicious Software in the Supplier System; and (f) 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: (i) was part of a wider effort to access information and communications technology operated by or on behalf of Central Government Bodies; or (ii) was undertaken, or directed by, a state other than the United Kingdom;
"Buyer Equipment"	any hardware, computer or telecoms devices, and equipment that forms part of the Buyer System;
"Buyer Security Policies"	those security policies specified by the Buyer in Paragraph 1.3;
"Buyer System"	the Buyer's information and communications technology system, including any software or Buyer Equipment, owned by the Buyer or leased or licenced to it by a third-party, that: (a) is used by the Buyer or Supplier in connection with this Contract; (b) interfaces with the Supplier System; and/or (c) is necessary for the Buyer to receive the Services;
"Certifications"	one or more of the following certifications (or equivalent): (a) ISO/IEC 27001:2022 by a UKAS-recognised Certification Body in respect of the Supplier System, or in respect of a wider system of which the Supplier System forms part; and (b) Cyber Essentials Plus; and/or (c) Cyber Essentials;
"CHECK Scheme"	the NCSC's scheme under which approved companies can conduct authorised penetration tests of public sector and critical national infrastructure systems and networks;
"CHECK Service Provider"	a company which, under the CHECK Scheme: (a) has been certified by the NCSC; (b) holds "Green Light" status; and (c) is authorised to provide the IT Health Check services required by Paragraph 3.2 (*Security Testing*) of Part B *(Additional Requirements)*;

"Cloud Security Principles"	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-security/ implementing-the-cloud-security-principles;
"CREST Service Provider"	a company with an information security accreditation of a security operations centre qualification from CREST International;
"Cyber Essentials"	the Cyber Essentials certificate issued under the Cyber Essentials Scheme;
"Cyber Essentials Plus"	the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme;
"Cyber Essentials Scheme"	the Cyber Essentials scheme operated by the NCSC;
"End-User Device"	any personal computers, laptops, tablets, terminals, smartphones or other portable electronic device provided by the Supplier or a Sub-contractor and used in the provision of the Services;
"Expected Behaviours"	the expected behaviours set out and updated from time to time in the Government Security Classification Policy, currently found at paragraphs 2 to 6 and in the table below paragraph 6 of https://www.gov.uk/government/publications/government-security-classifications/guidance-11-working-at-official-html;
"Government Data"	any: (a) data, texts, 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 Buyer is a, or the, Data Controller; or (c) any meta-data relating to categories of data referred to in Paragraphs (a) or (b) of this definition; that is: (d) supplied to the Supplier by or on behalf of the Buyer; or (e) that the Supplier is required to generate, process, Handle, store or transmit under this Contract;
"Government Security Classification Policy"	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;
"Handle"	eans 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;
"IT Health Check"	the security testing of the Supplier System;

"Malicious Software"	any software program or code intended to destroy, interfere with, corrupt, remove, transmit or cause undesired effects on program files, data or other information, executable code, applications, macros or configurations;
"NCSC"	the National Cyber Security Centre, or any successor body performing the functions of the National Cyber Security Centre;
"NCSC Device Guidance"	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;
"Privileged User"	a user with system administration access to the Supplier System, or substantially similar access privileges;
"Prohibition Notice"	the meaning given to that term by Paragraph 5.4;
"Protective Monitoring System"	has the meaning given to that term by Paragraph 7.1 of Part B *(Additional Requirements)*;
"Relevant Conviction"	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 Buyer may specify;
"Remote Location"	[the relevant Supplier Staff's permanent home address authorised by the Supplier or Sub-contractor (as applicable) for Remote Working OR a location other than a Supplier's or a Sub-contractor's Site];
"Remote Working"	the provision or management of the Services by Supplier Staff from a location other than a Supplier's or a Sub-contractor's Site;
"Remote Working Policy"	the policy prepared and approved under Paragraph 13 of Part B *(Additional Requirements)* under which Supplier Staff are permitted to undertake Remote Working;
"Security Controls"	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;
"Sites"	any premises (including the Buyer's Premises, the Supplier's premises or third party premises): (a) from, to or at which: (i) the Services are (or are to be) provided; or (ii) the Supplier manages, organises or otherwise directs the provision or the use of the Services; or (b) where: (i) any part of the Supplier System is situated; or (ii) any physical interface with the Buyer System takes place;

"Sub-contractor"	for the purposes of this Annex 6 *(Security Management)* only, any individual or entity that: (a) forms part of the supply chain of the Supplier; and (b) has access to, hosts, or performs any operation on or in respect of the Supplier System and the Government Data, and this definition shall apply to this Annex 6 in place of the definition of Sub-contractor in clause 1 of the Conditions *(Definitions)*;
"Supplier Staff"	for the purposes of this Annex 6 *(Security Management)* only, any individual engaged, directly or indirectly, or employed by the Supplier or any Sub-contractor (as that term is defined for the purposes of this Annex 6 *(Security Management)* only) in the management or performance of the Supplier's obligations under this Contract, and this definition shall apply to this Annex 6 *(Security Management*) in place of the definition of Supplier Staff in clause 1 of the Conditions *(Definitions)*;
"Supplier System"	(a) any: (i) information assets, (ii) IT systems, (iii) IT services; or (iv) Sites, that the Supplier or any Sub-contractor will use to Handle, or support the Handling of, Government Data and provide, or support the provision of, the Services; and (b) the associated information management system, including all relevant: (i) organisational structure diagrams; (ii) controls; (iii) policies; (iv) practices; (v) procedures; (vi) processes; and (vii) resources;
"Third-party Tool"	any software used by the Supplier by which the Government Data is accessed, analysed or modified, or some form of operation is performed on it; and
"UKAS-recognised Certification Body"	(a) an organisation accredited by UKAS to provide certification of ISO/IEC27001:2013 and/or ISO/IEC27001:2022; or (b) 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.

Part A Core Requirements

3 HANDLING GOVERNMENT DATA

3.1 The Supplier acknowledges that it:

3.1.1 must only Handle Government Data that is classified as OFFICIAL; and

3.1.2 must not Handle Government Data that is classified as SECRET or TOP SECRET.

3.2 The Supplier must:

3.2.1 not alter the classification of any Government Data.

3.2.2 if it becomes aware that it has Handled any Government Data classified as SECRET or TOP SECRET the Supplier must:

3.2.2.1 immediately inform the Buyer; and

3.2.2.2 follow any instructions from the Buyer concerning the Government Data.

3.3 The Supplier must, and must ensure that Sub-contractors and Supplier Staff, when Handling Government Data, comply with:

3.3.1 the Expected Behaviours; and

3.3.2 the Security Controls.

4 CERTIFICATION REQUIREMENTS

4.1 Where the Buyer has not specified Certifications under Paragraph 1.2, the Supplier must ensure that it and any Sub-contractors that Handle Government Data are certified as compliant with Cyber Essentials (or equivalent).

4.2 Where the Buyer has specified Certifications under Paragraph 1.2, the Supplier must ensure that both:

4.2.1 it; and

4.2.2 any Sub-contractor that Handles Government Data,

are certified as compliant with the Certifications specified by the Buyer in Paragraph 1.2 (or equivalent certifications):

4.3 The Supplier must ensure that the specified Certifications (or their equivalent) are in place for it and any relevant Sub-contractor:

4.3.1 before the Supplier or any Sub-contractor Handles Government Data; and

4.3.2 throughout the Term.

5 LOCATION

5.1 Where the Buyer has not specified any locations or territories in Paragraph 1.2, the Supplier must not, and ensure that Subcontractors do not store, access or Handle Government Data outside:

5.1.1 the United Kingdom; or

5.1.2 a location 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).

5.2 Where the Buyer has specified locations or territories in Paragraph 1.2, the Supplier must, and ensure that all Sub-contractors, at all times store, access or Handle Government Data only in or from the geographic areas specified by the Buyer.

5.3 The Supplier must, and must ensure that its Sub-contractors store, access or Handle Government Data in a facility operated by an entity where:

5.3.1 the entity has entered into a binding agreement with the Supplier or Sub-contractor (as applicable);

5.3.2 that binding agreement includes obligations on the entity in relation to security management at least an onerous as those relating to Sub-contractors in this Annex;

5.3.3 the Supplier or Sub-contractor has taken reasonable steps to assure itself that:

5.3.3.1 the entity complies with the binding agreement; and

5.3.3.2 the Sub-contractor's system has in place appropriate technical and organisational measures to ensure that the Sub-contractor will store, access, manage and/or Handle the Government Data as required by this Annex;

5.3.4 the Buyer has not given the Supplier a Prohibition Notice under Paragraph 5.4.

5.4 The Buyer may by notice in writing at any time give notice to the Supplier that it and its Sub-contractors must not undertake or permit to be undertaken the storage, accessing or Handling of Government Data in one or more countries or territories (a "**Prohibition Notice**").

5.5 Where the Supplier must and must ensure Sub-contractors comply with the requirements of a Prohibition Notice within 40 Working Days of the date of the notice.

6 STAFF VETTING

6.1 The Supplier must not allow, and must ensure that Sub-contractors do not allow Supplier Staff, to access or Handle Government Data, if that person has not undergone:

6.1.1 the checks required for the BPSS to verify:

6.1.1.1 the individual's identity;

6.1.1.2 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;

6.1.1.3 the individual's previous employment history; and

6.1.1.4 that the individual has no Relevant Convictions; and

6.1.2 national security vetting clearance to the level specified by the Authority for such individuals or such roles as the Authority may specify; or

6.1.3 such other checks for the Supplier Staff as the Buyer may specify.

6.2 Where the Supplier considers it cannot ensure that a Sub-contractor will undertake the relevant security checks on any Sub-contractor Staff, it must:

6.2.1 as soon as practicable, and in any event within 20 Working Days of becoming aware of the issue, notify the Buyer;

6.2.2 provide such information relating to the Sub-contractor, its vetting processes and the roles the affected Sub-contractor staff will perform as the Buyer reasonably requires; and

6.2.3 comply, at the Supplier's cost, with all directions the Buyer may provide concerning the vetting of the affected Sub-contractor Staff and the management of the Sub-contract.

7 SUPPLIER ASSURANCE LETTER

7.1 The Supplier must, no later than the last day of each Contract Year, provide to the Buyer a letter from its [chief technology officer] (or equivalent officer) confirming that, having made due and careful enquiry:

7.1.1 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;

7.1.2 it has fully complied with all requirements of this Annex; and

7.1.3 all Sub-contractors have complied with the requirements of this Annex with which the Supplier is required to ensure they comply;

7.1.4 the Supplier considers that its security and risk mitigation procedures remain effective.

8 ASSURANCE

8.1 The Supplier must provide such information and documents as the Buyer may request in order to demonstrate the Supplier's and any Sub-contractors' compliance with this Annex.

8.2 The Supplier must provide that information and those documents:

8.2.1 at no cost to the Buyer;

8.2.2 within 10 Working Days of a request by the Buyer;

8.2.3 except in the case of original document, in the format and with the content and information required by the Buyer; and

8.2.4 in the case of original document, as a full, unedited and unredacted copy.

9 USE OF SUB-CONTRACTORS AND THIRD PARTIES

9.1 The Supplier must ensure that Sub-contractors and any other third parties that store, have access to or Handle Government Data comply with the requirements of this Annex.

Part B Additional Requirements

1 SECURITY MANAGEMENT PLAN

1.1 This Paragraph 1 of Part B *(Additional Requirements)* applies only where the Buyer has selected this option in Paragraph 1.3.

Preparation of Security Management Plan

1.2 The Supplier shall document in the Security Management Plan how the Supplier and its Sub-contractors shall comply with the requirements set out in this Annex and the Contract in order to ensure the security of the Supplier solution and the Buyer data.

1.3 The Supplier shall prepare and submit to the Buyer within 20 Working Days of the date of this Contract, the Security Management Plan, which must include a description of how all the options selected in this Annex are being met along with evidence of the required certifications for the Supplier and any Sub-contractors specified in Paragraph 4 of Part B *(Additional Requirements)*.

Approval of Security Management Plan

1.4 The Buyer shall review the Supplier's proposed Security Management Plan as soon as possible and must issue the Supplier with either:

1.4.1 an information security approval statement, which shall confirm that the Supplier may operate the service and process Buyer data; or

1.4.2 a rejection notice, which shall set out the Buyer's reasons for rejection the Security Management Plan.

1.5 If the Buyer rejects the Supplier's proposed Security Management Plan, the Supplier must prepare a revised Security Management Plan taking the Buyer's reasons into account, which the Supplier must submit to the Buyer for review within 10 Working Days of the date of the rejection, or such other period agreed with the Buyer.

1.6 The process set out in Paragraph 1.5 of Part B *(Additional Requirements)* shall be repeated until such time as the Authority issues a Risk Management Approval Statement to the Supplier or terminates this Contract.

1.7 The rejection by the Buyer of a second revised Security Management Plan is a material Default of this Contract.

Updating Security Management Plan

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

Monitoring

1.9 The Supplier shall notify the Buyer within 2 Working Days after becoming aware of:

1.9.1 a significant change to the components or architecture of the Supplier System;

1.9.2 a new risk to the components or architecture of the Supplier System;

1.9.3 a vulnerability to the components or architecture of the Supplier System using an industry standard vulnerability scoring mechanism;

1.9.4 a change in the threat profile;

1.9.5 a significant change to any risk component;

1.9.6 a significant change in the quantity of Personal Data held within the Service;

1.9.7 a proposal to change any of the Sites from which any part of the Services are provided; and/or

1.9.8 an ISO27001 audit report produced in connection with the Certification indicates significant concerns.

1.10 Within 10 Working Days of such notifying the Buyer or such other timescale as may be agreed with the Buyer, the Supplier shall make the necessary changes to the Security Management Plan and submit the updated Security Management Plan to the Buyer for review and approval.

2 BUYER SECURITY POLICIES

2.1 The Supplier must comply, when it provides the Services and operates and manages the Supplier System, with all Buyer Security Policies identified in the relevant option in Paragraph 1.3.

2.2 If there is an inconsistency between the Buyer Security Policies and the requirement of this Annex, then the requirements of this Annex will prevail to the extent of that inconsistency.

3 SECURITY TESTING

3.1 The Supplier must:

3.1.1 before Handling Government Data;

3.1.2 at least once during each Contract Year; and

3.1.3 undertake the following activities:

3.1.3.1 conduct security testing of the Supplier System (an "**IT Health Check**") in accordance with Paragraph 3.2 of this Part B *(Additional Requirements)*; and

3.1.3.2 implement any findings, and remedy any vulnerabilities identified by the IT Health Check in accordance with Paragraph 3.3 of this Part B *(Additional Requirements)*.

3.2 In arranging an IT Health Check, the Supplier must:

3.2.1 use only a CHECK Service Provider or CREST Service Provider to perform the IT Health Check;

3.2.2 design and plan for the IT Health Check so as to minimise the impact of the IT Health Check on the Supplier System and the delivery of the Services;

3.2.3 ensure that the scope of the IT Health Check encompasses the components of the Supplier System used to access, store, Handle or manage Government Data; and

3.2.4 ensure that the IT Health Check provides for effective penetration testing of the Supplier System.

3.3 The Supplier treat any vulnerabilities as follows:

3.3.1 the Supplier must remedy any vulnerabilities classified as high in the IT Health Check report:

3.3.1.1 if it is technically feasible to do so, within 5 Working Days of becoming aware of the vulnerability and its classification; or

3.3.1.2 if it is technically feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 3.3.1.1, then as soon as reasonably practicable after becoming aware of the vulnerability and its classification;

3.3.2 the Supplier must remedy any vulnerabilities classified as high in the IT Health Check report:

3.3.2.1 if it is technically feasible to do so, within 1 month of becoming aware of the vulnerability and its classification; or

3.3.2.2 if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 3.3.2.1, then as soon as reasonably practicable after becoming aware of the vulnerability and its classification;

3.3.3 the Supplier must remedy any vulnerabilities classified as medium in the IT Heath Check report:

3.3.3.1 if it is technically feasible to do so, within 3 months of becoming aware of the vulnerability and its classification; or

3.3.3.2 if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 3.3.3.1, then as soon as reasonably practicable after becoming aware of the vulnerability and its classification; and

3.3.4 where it is not technically feasible to remedy the vulnerability, the Supplier must implement appropriate technical and organisational measures to mitigate the risk posed by the vulnerability.

4 CLOUD SECURITY PRINCIPLES

4.1 The Supplier must ensure that the Supplier System complies with the Cloud Security Principles.

4.2 The Supplier must assess the Supplier System against the Cloud Security Principles to assure itself that it complies with Paragraph 4.1 of this Part B *(Additional Requirements)*:

4.2.1 before Handling Government Data;

4.2.2 at least once each Contract Year; and

4.2.3 when required by the Buyer.

4.3 Where the Cloud Security Principles provide for various options, the Supplier must document the option it has chosen to implement and its reasons for doing do.

4.4 The Supplier must:

4.4.1 keep records of any assessment that it makes under Paragraph 4.2 of this Part B *(Additional Requirements)*; and

4.4.2 provide copies of those records to the Buyer within 10 Working Days of any request by the Buyer.

5 INFORMATION ABOUT SUB-CONTRACTORS, SITES AND THIRD-PARTY TOOLS

5.1 The Supplier must keep the following records:

5.1.1 for Sub-contractors or third parties that store, have access to or Handle Government Data:

5.1.1.1 the Sub-contractor or third party's name:

(a) legal name;

(b) trading name (if any); and

(c) registration details (where the Sub-contractor is not an individual), including:

i. country of registration;

ii. registration number (if applicable); and

iii. registered address;

(d) the Certifications held by the Sub-contractor or third party;

(e) the Sites used by the Sub-contractor or third party;

(f) the Services provided or activities undertaken by the Sub-contractor or third party;

(g) the access the Sub-contractor or third party has to the Supplier System;

(h) the Government Data Handled by the Sub-contractor or third party; and

(i) the measures the Sub-contractor or third party has in place to comply with the requirements of this Annex;

5.1.1.2 for Sites from or at which Government Data is accessed or Handled:

(a) the location of the Site;

(b) the operator of the Site, including the operator's:

i. legal name;

ii. trading name (if any); and

iii. registration details (where the Sub-contractor is not an individual);

iv. the Certifications that apply to the Site;

v. the Government Data stored at, or Handled from, the site; and

5.1.1.3 for Third-party Tools:

(a) the name of the Third-Party Tool;

5.1.1.4 the nature of the activity or operation performed by the Third-Party Tool on the Government Data; and

(a) in respect of the entity providing the Third-Party Tool, its:

i. full legal name;

ii. trading name (if any)

iii. country of registration;

iv. registration number (if applicable); and

v. registered address.

5.2 The Supplier must update the records it keeps in accordance with Paragraph 5.1 of this Part B *(Additional Requirements)*:

5.2.1 at least four times each Contract Year;

5.2.2 whenever a Sub-contractor, third party that accesses or Handles Government Data, Third-party Tool or Site changes; or

5.2.3 whenever required to do so by the Buyer.

5.3 The Supplier must provide copies of the records it keeps in accordance with Paragraph 5.1 of this Part B *(Additional Requirements)* to the Buyer within 10 Working Days of any request by the Buyer.

6 ENCRYPTION

6.1 The Supplier must, and must ensure that all Sub-contractors, encrypt Government Data:

6.1.1 when stored at any time when no operation is being performed on it, including when stored on any portable storage media; and

6.1.2 when transmitted.

7 PROTECTIVE MONITORING SYSTEM

7.1 The Supplier must, and must ensure that Sub-contractors, implement an effective system of monitoring and reports, analysing access to and use of the Supplier System and the Government Data to:

7.1.1 identify and prevent any potential Breach of Security;

7.1.2 respond effectively and in a timely manner to any Breach of Security that does;

7.1.3 identify and implement changes to the Supplier System to prevent future any Breach of Security; and

7.1.4 help detect and prevent any potential criminal offence relating to fraud, bribery or corruption using the Supplier System,

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

7.2 The Protective Monitoring System must provide for:

7.2.1 event logs and audit records of access to the Supplier System; and

7.2.2 regular reports and alerts to identify:

7.2.2.1 changing access trends;

7.2.2.2 unusual usage patterns; or

7.2.2.3 the access of greater than usual volumes of Government Data; and

7.2.2.4 the detection and prevention of any attack on the Supplier System using common cyber-attack techniques.

8 PATCHING

8.1 The Supplier must, and must ensure that Sub-contractors, treat any public releases of patches for vulnerabilities as follows:

8.1.1 the Supplier must patch any vulnerabilities classified as "**critical**":

8.1.1.1 if it is technically feasible to do so, within 5 Working Days of the public release; or

8.1.1.2 if it is technical feasible to patch the vulnerability but not technically feasible to do so as required by Paragraph 8.1.1.1, then as soon as reasonably practicable after the public release;

8.1.2 the Supplier must patch any vulnerabilities classified as "**important**":

8.1.2.1 if it is technically feasible to do so, within 1 month of the public release; or

8.1.2.2 if it is technical feasible to patch the vulnerability but not technically feasible to do so as required by Paragraph 8.1.2.1, then as soon as reasonably practicable after the public release;

8.1.3 the Supplier must remedy any vulnerabilities classified as "**other**" in the public release:

8.1.3.1 if it is technically feasible to do so, within 2 months of the public release; or

8.1.3.2 if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 8.1.3.1, then as soon as reasonably practicable after the public release;

8.1.4 where it is not technically feasible to patch the vulnerability, the Supplier must implement appropriate technical and organisational measures to mitigate the risk posed by the vulnerability.

9 MALWARE PROTECTION

9.1 The Supplier shall install and maintain Anti-virus Software or procure that Anti-virus Software is installed and maintained on the Supplier System.

9.2 The Supplier must ensure that such Anti-virus Software:

9.2.1 prevents the installation of the most common forms of Malicious Software in the Supplier System;

9.2.2 performs regular scans of the Supplier System to check for Malicious Software; and

9.2.3 where Malicious Software has been introduced into the Supplier System, so far as practicable

9.2.3.1 prevents the harmful effects from the Malicious Software; and

9.2.3.2 removes the Malicious Software from the Supplier System.

10 END-USER DEVICES

10.1 The Supplier must, and must ensure that all Sub-contractors, manage all End-User Devices on which Government Data is stored or Handled in accordance with the following requirements:

10.1.1 the operating system and any applications that store, Handle or have access to Government Data must be in current support by the vendor, or the relevant community in the case of open source operating systems or applications;

10.1.2 users must authenticate before gaining access;

10.1.3 all Government Data must be encrypted using a suitable encryption tool;

10.1.4 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;

10.1.5 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 to ensure the security of that Government Data;

10.1.6 the Supplier or Sub-contractor, as applicable, can, without physical access to the End-User Device, remove or make inaccessible all Government Data stored on the device and prevent any user or group of users from accessing the device;

10.1.7 all End-User Devices are within the scope of any required Certification.

10.2 The Supplier must comply, and ensure that all Sub-contractors comply, with the recommendations in NCSC Device Guidance as if those recommendations were incorporated as specific obligations under this Contract.

11 VULNERABILITY SCANNING

11.1 The Supplier must:

11.1.1 scan the Supplier System at least once every month to identify any unpatched vulnerabilities; and

11.1.2 if the scan identifies any unpatched vulnerabilities, ensure they are patched in accordance with Paragraph 8 of this Part B *(Additional Requirements)*.

12 ACCESS CONTROL

12.1 The Supplier must, and must ensure that all Sub-contractors:

12.1.1 identify and authenticate all persons who access the Supplier System before they do so;

12.1.2 require multi-factor authentication for all user accounts that have access to Government Data or that are Privileged Users;

12.1.3 allow access only to those parts of the Supplier System and Sites that those persons require; and

12.1.4 maintain records detailing each person's access to the Supplier System.

12.2 The Supplier must ensure, and must ensure that all Sub-contractors ensure, that the user accounts for Privileged Users of the Supplier System:

12.2.1 are allocated to a single, individual user;

12.2.2 are accessible only from dedicated End-User Devices;

12.2.3 are configured so that those accounts can only be used for system administration tasks;

12.2.4 require passwords with high complexity that are changed regularly;

12.2.5 automatically log the user out of the Supplier System after a period of time that is proportionate to the risk environment during which the account is inactive; and

12.2.6 are:

12.2.6.1 restricted to a single role or small number of roles;

12.2.6.2 time limited; and

12.2.6.3 restrict the Privileged User's access to the internet.

13 REMOTE WORKING

13.1 The Supplier must ensure, and ensure that Sub-contractors ensure, that:

13.1.1 unless in writing by the Authority, Privileged Users do not undertake Remote Working;

13.1.2 where the Authority permits Remote Working by Privileged Users, the Supplier ensures, and ensures that Sub-contractors ensure, that such Remote Working takes place only in accordance with any conditions imposed by the Authority.

13.2 Where the Supplier or a Sub-contractor wishes to permit Supplier Staff to undertake Remote Working, it must:

13.2.1 prepare and have approved by the Buyer in the Remote Working Policy in accordance with this Paragraph;

13.2.2 undertake and, where applicable, ensure that any relevant Sub-contractors undertake, all steps required by the Remote Working Policy;

13.2.3 ensure that Supplier Staff undertake Remote Working only in accordance with the Remote Working Policy;

13.2.4 may not permit any Supplier Staff or the Supplier or any Sub-contractor to undertake Remote Working until the Remote Working Policy is approved by the Buyer.

13.3 The Remote Working Policy must include or make provision for the following matters:

13.3.1 restricting or prohibiting Supplier Staff from printing documents in any Remote Location;

13.3.2 restricting or prohibiting Supplier Staff from downloading any Government Data to any End-User Device other than an End User Device that:

13.3.2.1 is provided by the Supplier or Sub-contractor (as appropriate); and

13.3.2.2 complies with the requirements set out in Paragraph 10 (*End-User Devices*) of this Part B *(Additional Requirements)*;

13.3.3 ensuring that Supplier Staff comply with the Expected Behaviours (so far as they are applicable);

13.3.4 giving effect to the Security Controls (so far as they are applicable); and

13.3.5 for each different category of Supplier Staff subject to the proposed Remote Working Policy:

13.3.5.1 the types and volumes of Government Data that the Supplier Staff can Handle in a Remote Location and the Handling that those Supplier Staff will undertake;

13.3.5.2 any identified security risks arising from the proposed Handling in a Remote Location;

13.3.5.3 the mitigations, controls and security measures the Supplier or Sub-contractor (as applicable) will implement to mitigate the identified risks; and

13.3.5.4 the business rules with which the Supplier Staff must comply.

13.4 The Supplier may submit a proposed Remote Working Policy for consideration at any time.

14 BACKUP AND RECOVERY OF GOVERNMENT DATA

14.1 The Supplier must ensure that the Supplier System:

14.1.1 backs up and allows for the recovery of Government Data to achieve the recovery point and recovery time objectives specified by the Buyer, or in accordance with Good Industry Practice where the Buyer has not specified; and

14.1.2 retains backups of the Government Data for the period specified by the Buyer, or in accordance with Good Industry Practice where the Buyer has not specified.

14.2 The Supplier must ensure the Supplier System:

14.2.1 uses backup location for Government Data that are physically and logically separate from the rest of the Supplier System;

14.2.2 the backup system monitors backups of Government Data to:

14.2.2.1 identify any backup failure; and

14.2.2.2 confirm the integrity of the Government Data backed up;

14.2.3 any backup failure is remedied properly;

14.2.4 the backup system monitors backups of Government Data to:

14.2.4.1 identify any recovery failure; and

14.2.4.2 confirm the integrity of Government Data recovered; and

14.2.5 any recovery failure is promptly remedied.

15 RETURN AND DELETION OF GOVERNMENT DATA

15.1 Subject to Paragraph 15.2 of this Part B *(Additional Requirements)*, when requested to do so by the Buyer, the Supplier must, and must ensure that all Sub-contractors:

15.1.1 securely erase any or all Government Data held by the Supplier or Sub-contractor using a deletion method that ensures that even a determined expert using specialist techniques can recover only a small fraction of the data deleted; or

15.1.2 provide the Buyer with copies of any or all Government Data held by the Supplier or Sub-contractor using the method specified by the Buyer.

15.2 Paragraph 15.1 of this Part B *(Additional Requirements)* does not apply to Government Data:

15.2.1 that is Personal Data in respect of which the Supplier is a Controller;

15.2.2 to which the Supplier has rights to Handle independently from this Contract; or

15.2.3 in respect of which, the Supplier is under an obligation imposed by Law to retain.

15.3 The Supplier must, and must ensure that all Sub-contractors, provide the Buyer with copies of any or all Buyer Data held by the Supplier or Sub-contractor:

15.3.1 when requested to do so by the Buyer; and

15.3.2 using the method specified by the Buyer.

16 PHYSICAL SECURITY

16.1 The Supplier must, and must ensure that Sub-contractors, store the Government Data on servers housed in physically secure locations.

17 BREACH OF SECURITY

17.1 If the Supplier becomes aware of a Breach of Security that impacts or has the potential to impact the Government Data, it shall:

17.1.1 notify the Buyer as soon as reasonably practicable after becoming aware of the breach, and in any event within [24] hours;

17.1.2 provide such assistance to the Buyer as the Buyer requires until the Breach of Security and any impacts or potential impacts on the Buyer are resolved to the Buyer's satisfaction; and

17.1.3 where the Law requires the Buyer to report a Breach of Security to the appropriate regulator provide such information and other input as the Buyer requires within the timescales specified by the Buyer.