

Call-Off Schedule 9E (Security: Buyer-led Assurance)

[Buyer Guidance: Buyers may include their own security requirements in the Call-Off Order Form, or use one of the optional Security Schedules listed below. See the separate Guidance Document (<https://www.security.gov.uk/policy-and-guidance/contracting-securely/>) about when to use an optional Security Schedule, and what version of the Security Schedule is most appropriate. Buyers can only choose one of the following Security Schedules, which will need to be completed (in line with the Buyer guidance set out in each document) and then referred to in the Call-Off Order Form:

- **Call-Off Schedule 9A (Security: Short Form)**
- **Call-Off Schedule 9B (Security: Consultancy)**
- **Call-Off Schedule 9C (Security: Development)**
- **Call-Off Schedule 9D (Security: Supplier-led Assurance)**
- **Call-Off Schedule 9E (Security: Buyer-led Assurance)**

Please note that certain information will need to be populated/confirmed by Buyers within the provisions of this Schedule in order to reflect the Buyer's own specific policies/requirements – the relevant provisions are highlighted in yellow.]

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

1. Buyer Options

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:

Buyer Security Policies (see Paragraph 5)		
The Buyer requires the Supplier to comply with the following policies relating to security management: <ul style="list-style-type: none">[Buyer Guidance: List Buyer security policies with which the Supplier and Sub-contractors must comply]	<input type="checkbox"/>	
Secure by Design Principles (see Paragraph 14.6)		
The Buyer waives the requirement for the Security Management Plan to include an assessment of the Supplier Information Management System against the table in Appendix 5 (<i>Secure by Design Principles Evaluation Table</i>).	<input type="checkbox"/>	
Locations (see Paragraph 1 of Appendix 1)		
The Supplier and Sub-contractors may store, access or Handle Government Data in: [Buyer Guidance: Include an "X" against the applicable item in the final column opposite]	the United Kingdom only	<input type="checkbox"/>
	any territory as permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State)	<input type="checkbox"/>
	anywhere in the world not prohibited by the Buyer [Buyer Guidance: Where selecting this option Buyers should review the Cabinet Office list of prohibited countries and any other Buyer specific policies and agree with the Supplier a written list of permitted locations prior to the Supplier commencing any activities]	<input type="checkbox"/>
Support Locations (see Paragraph 1 of Appendix 1)		
	the United Kingdom only	<input type="checkbox"/>

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

The Supplier and Sub-contractors may operate Support Locations in: [Buyer Guidance: Include an "X" against the applicable item in the final column opposite]	any territory as permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State)	<input type="checkbox"/>
	anywhere in the world not prohibited by the Buyer	<input type="checkbox"/>
Development Activity (see Appendix 2)		
The Buyer requires the Supplier to undertake Development Activity under the Contract and, as a consequence, Appendix 2 applies [Buyer Guidance: Include an "X" in the final column opposite if Development Activity is required, or leave blank if no Development Activity is required]		<input type="checkbox"/>
Locations for Development Activity (applies only if the option relating to Development Activities is selected; see Paragraph 1 of Appendix 1) [Buyer Guidance: Include an "X" against the applicable item in the final column opposite, only if Development Activity is required as confirmed in the preceding row]		
The Supplier and Sub-contractors may undertake Development Activity in:	the United Kingdom only	<input type="checkbox"/>
	any territory as permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State)	<input type="checkbox"/>
	anywhere in the world not prohibited by the Buyer	<input type="checkbox"/>

2. Definitions

- 2.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (*Definitions*):

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

"Anti-virus Software"	<p>software that:</p> <ul style="list-style-type: none">(a) protects the Supplier Information Management System from the possible introduction of Malicious Software;(b) scans for and identifies possible Malicious Software in the Supplier Information Management System;(c) if Malicious Software is detected in the Supplier Information Management System, so far as possible:<ul style="list-style-type: none">(i) prevents the harmful effects of the Malicious Software; and(ii) removes the Malicious Software from the Supplier Information Management System;
"Assets"	<p>all assets and rights used by the Supplier to provide the Services in accordance with the Contract but excluding the Buyer Assets;</p>
"Buyer-led Assurance"	<p>the assessment of the Supplier Information Management System in accordance with Paragraph 15 by the Buyer or an independent information risk manager or other qualified professional appointed by the Buyer;</p>
"Backup and Recovery Plan"	<p>the section of the Security Management Plan setting out the Suppliers' and Sub-contractors' plans for the back and recovery of any Government Data they Handle;</p>
"Breach Action Plan"	<p>a plan prepared under Paragraph 16.3 of Appendix 1 addressing any Breach of Security;</p>
"Breach of Security"	<p>the occurrence of:</p> <ul style="list-style-type: none">(a) any unauthorised access to or use of the Services, the Buyer Premises, the Sites, the Supplier Information Management System and/or any information or data used by the Buyer, the Supplier or any Sub-contractor in connection with the Contract, including the Government Data and the Code;(b) the loss (physical or otherwise), corruption and/or unauthorised disclosure of any information or data, including copies of such information or data, used by the Buyer, the Supplier or any Sub-contractor in

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

	connection with the Contract, including the Government Data and the Code; and/or
	(c) any part of the Supplier Information Management System ceasing to be compliant with the Certification Requirements;
	(d) the installation of Malicious Software in the: <ul style="list-style-type: none">(i) Supplier Information Management System;(ii) Development Environment; or(iii) Developed 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: <ul style="list-style-type: none">(i) Supplier Information Management System;(ii) Development Environment; or(iii) Developed System; and
	(f) includes any attempt to undertake the activities listed in sub-Paragraph (a) where the Supplier has reasonable grounds to suspect that attempt: <ul style="list-style-type: none">(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;
"Certification Requirements"	the requirements set out in Paragraph 13.3;
"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: <ul style="list-style-type: none">(a) has been certified by the National Cyber Security Centre;(b) holds "Green Light" status; and(c) is authorised to provide the IT Health Check services required by Paragraph 12 of Appendix 1;

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

"CHECK Team Leader"	an individual with a CHECK Scheme team leader qualification issued by the NCSC;
"CHECK Team Member"	an individual with a CHECK Scheme team member qualification issued by the NCSC;
"Code Review"	<p>a periodic review of the Code by manual or automated means to:</p> <ul style="list-style-type: none">(a) identify and fix any bugs; and(b) ensure the Code complies with<ul style="list-style-type: none">(i) the requirements of this Schedule (Security); and(ii) the Secure Development Guidance;
"Code Review Plan"	the document agreed with the Buyer under Paragraph 5.2 of the security requirements for Development Activity in Appendix 2 setting out the requirements for, and frequency of, Code Reviews;
"Code Review Report"	a report setting out the findings of a Code Review;
"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 National Cyber Security Centre;
"Data Migration Plan"	the plan for the migration of the Government Data to the Buyer and/or the Replacement Supplier (as required by the Buyer) required by Paragraph 17 of Appendix 1;
"Development Activity"	<p>any activity relating to the development, deployment maintenance and upgrading of the Developed System, including:</p> <ul style="list-style-type: none">(a) coding;(b) testing;(c) code storage; and(d) deployment;

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

"Development Environment"	any information and communications technology system and the Sites forming part of the Supplier Information Management System that the Supplier or its Sub-contractors will use to provide the Development Activity;
"EEA"	the European Economic Area;
"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;
"Email Service"	a service that will send, or can be used to send, emails from the Buyer's email address or otherwise on behalf of the Buyer;
"Expected Behaviours"	the expected behaviours set out and updated from time to time in the Government Security Classification Policy, currently found at paragraphs 12 to 16 and in the table below paragraph 16 of https://www.gov.uk/government/publications/government-security-classifications/guidance-11-working-at-official-html ;
"Government Data Register"	the register of all Government Data the Supplier, or any Sub-contractor, receives from or creates for the Buyer, produced and maintained in accordance with Paragraph 18 of Appendix 1;

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

"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>;

"Higher-risk Sub-contractor"

a Sub-contractor that Handles Government Data, where that data includes either:

- (a) the Personal Data of 1000 or more individuals in aggregate during the period between the Start Date and the End Date4.1.2; or
- (b) any part of that Personal Data includes any of the following:
 - (i) financial information (including any tax and/or welfare information) relating to any person;
 - (ii) any information relating to actual or alleged criminal offences (including criminal records);
 - (iii) any information relating to children and/or vulnerable persons;
 - (iv) any information relating to social care;
 - (v) any information relating to a person's current or past employment; or
 - (vi) Special Category Personal Data; or
- (c) the Buyer in its discretion, designates a Sub-contractor as a Higher- risk Sub-contractor:
 - (i) in any procurement document related to the Contract; or
 - (ii) during the Contract Period;

"HMG Baseline Personnel Security Standard"

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;

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

"Independent Security Adviser"	the independent and appropriately qualified and experienced security architect or expert appointed under Paragraph 20;
"ISO Certification"	either of the following certifications when issued by a UKAS-recognised Certification Body: (a) ISO/IEC27001:2013, where the certification was obtained before November 2022, but only until November 2025; and (b) ISO/IEC27001:2022 in all other cases;
"IT Health Check"	testing of the Supplier Information Management System by a CHECK Service Provider;
"Key Subcontractor Default"	has the meaning set out in Paragraph 10.5;
"Medium-risk Sub-contractor"	a Sub-contractor that Handles Government Data, [where that data (a) includes the Personal Data of between 100 and 999 individuals (inclusive) in the period between the Start Date and the End Date4.1.2; and (b) does not include Special Category Personal Data];
"Modules Register"	the register of Third-party Software Modules required by Paragraph 7.3 of Appendix 1;
"NCSC"	the National Cyber Security Centre or any replacement or successor body carrying out the same function;
"NCSC 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/the-cloud-security-principles ;
"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 ;
"NCSC Protecting Bulk Personal Data Guidance"	the NCSC's document "Protecting Bulk Personal Data", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/protecting-bulk-personal-data ;

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

"NCSC Secure Design Principles"	the NCSC's document "Secure Design Principles", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cyber-security-design-principles/cyber-security-design-principles ;
"OWASP"	the Open Web Application Security Project Foundation;
"OWASP Secure Coding Practice"	the Secure Coding Practices Quick Reference Guide published by OWASP, as updated or replaced from time to time and found at https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/ ;
"OWASP Top Ten"	the list of the most critical security risks to web applications published annually by OWASP and found at https://owasp.org/www-project-top-ten/ ;
"Privileged User"	a user with system administration access to the Supplier Information Management System, or substantially similar access privileges;
"Prohibited Activity"	the storage, access or Handling of Government Data prohibited by a Prohibition Notice;
"Prohibition Notice"	a notice issued under Paragraph 1.11 of Appendix 1;
"Protective Monitoring System"	the system implemented by the Supplier and its Sub-contractors under Paragraph 14.1 of Appendix 1 to monitor and analyse access to and use of the Supplier Information Management System, the Development Environment, the Government Data and the Code;
"RAP Trigger"	the occurrence of one of the events set out in Paragraph 19.1;

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

"Register of Sites, Support Locations and Third-party Tools"

the part of the Security Management Plan setting out, in respect of Sites, Support Locations and Third-party Tools:

- (a) the Sites, Support Locations and Third-party Tools that the Supplier will use to Handle Government Data or provide the Services;
- (b) the nature of the activity performed at the Site or Support Location or by the Third-party Tool in respect of the Government Data;
- (c) in respect of each entity providing a Site, Support Location or 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;

"Relevant Activities"

those activities specified in Paragraph 1.1 of Appendix 1;

"Relevant Certifications"

- (a) in the case of the Supplier, any SIMS Sub-contractor and any Key Subcontractor:
 - (i) either:
 - (A) an ISO Certification in respect of the Supplier Information Management System; or
 - (B) where the Supplier Information Management System is included within the scope of a wider ISO Certification, that ISO Certification; and
 - (ii) Cyber Essentials Plus;
- (b) In the case of any Higher-risk Sub-contractor, either:
 - (i) an ISO Certification in respect of that part of the Supplier Information Management System provided by the Higher-risk Sub-contractor;
 - (ii) where the that part of the Supplier Information Management System provided by the Higher-risk Sub-contractor is included

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

	within the scope of a wider ISO Certification, that ISO Certification; or
	(iii) Cyber Essentials Plus; and
	(c) in the case of any Medium-risk Sub-contractors, Cyber Essentials.
	(or equivalent certifications);
"Relevant Convictions"	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;
"Remediation Action Plan"	the plan prepared by the Supplier in accordance with Paragraph 12.13 to 12.17, addressing the vulnerabilities and findings in a IT Health Check report;
"Remote Location"	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 3.8 of Appendix 1 and forming part of the Security Management Plan under which Supplier Staff are permitted to undertake Remote Working;
"Required Changes Register"	<p>the register recording each of the changes that the Supplier proposes to the Supplier Information Management System or the Security Management Plan together with:</p> <p>(a) the details of any approval of the change provided by the Buyer, including any conditions or limitations on that approval; and</p> <p>(b) the date:</p> <p>(i) the date by which the change is to be implemented; and</p> <p>(ii) the date on which the change was implemented;</p>
"Residual Risk Statement"	a notice issued by the Buyer that

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

	<ul style="list-style-type: none">(a) sets out the information risks associated with using the Supplier Information Management System; and(b) confirms that the Buyer:<ul style="list-style-type: none">(i) is satisfied that the identified risks have been adequately and appropriately addressed; and(ii) that the residual risks are understood and accepted by the Buyer;
"Risk Management Approval Statement"	the statement issued by the Buyer under Paragraph 15.7 following the Buyer-led Assurance of the Supplier Information Management System;
"Secure by Design Principles"	the Secure by Design Principles issued by the Cabinet Office, as updated or replaced from time-to-time, currently found at https://www.security.gov.uk/policy-and-guidance/secure-by-design/principles/ ;
"Secure Development Guidance"	the Supplier's secure coding policy required under its ISO27001 Relevant Certification.
"Secure Location"	has the meaning given to that term in Paragraph 2.1.1 of Appendix 1;
"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 ;
"Security Management Plan"	the document prepared in accordance with the requirements of Paragraph 14 and in the format, and containing the information, specified in [insert cross-reference to guidance] ;
"security requirements for Development Activity"	the security requirements in Appendix 2 to this Schedule;
"Security Test"	<ul style="list-style-type: none">(a) an IT Health Check; or(b) a Supplier Security Test;

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

"Security Working Group"	the Board established under Paragraph 8;
"SIMS Sub-contractor"	a Sub-contractor designated by the Buyer that provides or operates the whole, or a substantial part, of the Supplier Information Management System;
"SMP Sub-contractor"	a Sub-contractor that provides cloud-based services on a "one to many" basis, where such Sub-contractor will not contract other than on their own contractual terms;
"Statement of Information Risk Appetite"	<p>the statement provided by the Buyer under Paragraph 14.1 setting out:</p> <ul style="list-style-type: none">(a) the nature and level of risk that the Supplier accepts from the operation of the Supplier Information Management System; and(b) the specific legal and regulatory requirements with which the Supplier must comply when Handling Government Data;
"Sub-contractor"	<p>for the purposes of this Schedule only, any individual or entity that:</p> <ul style="list-style-type: none">(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 Information Management System, the Development Environment, the Code and the Government Data, <p>and this definition shall apply to this Schedule in place of the definition of Subcontractor in Joint Schedule 1 (<i>Definitions</i>);</p>
"Sub-contractors' Systems"	<p>the information and communications technology system used by a Sub-contractor in implementing and performing the Services, including:</p> <ul style="list-style-type: none">(a) the Software;(b) the Supplier Equipment;(c) configuration and management utilities;(d) calibration and testing tools;(e) and related cabling; but <p>does not include the Buyer System;</p>
"Supplier Information"	those parts of Wider Information Management System that the Buyer has determined in accordance with

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

"Management System"	Paragraph 11, following consultation with the Supplier, shall be subject to Buyer-led Assurance;
"Supplier Staff"	for the purposes of this Schedule 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 Schedule) in the management or performance of the Supplier's obligations under the Contract, and this definition shall apply to this Schedule in place of the definition of Supplier Staff in Joint Schedule 1 (<i>Definitions</i>);
"Support Location"	a place or facility where or from which individuals may access or Handle the Code or the Government Data;
"Support Register"	the register of all hardware and software used to provide the Services produced and maintained in accordance with Paragraph 5 of Appendix 1;
"Third-party Software Module"	<p>any module, library or framework that:</p> <ul style="list-style-type: none">(a) is not produced by the Supplier or a Sub-contractor as part of the Development Activity; and(b) either:<ul style="list-style-type: none">(i) forms, or will form, part of the Code; or(ii) is, or will be, accessed by the Developed System during its operation;
"Third-party Tool"	any Software used by the Supplier by which the Code or the Government Data is accessed, analysed or modified, or some form of operation is performed on it;
"UKAS"	the United Kingdom Accreditation Service;
"UKAS-recognised Certification Body"	<ul style="list-style-type: none">(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; and
"Wider Information Management System"	<ul style="list-style-type: none">(a) any:<ul style="list-style-type: none">(i) information assets,(ii) IT systems,

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

- (iii) IT services; or Sites
- that the Supplier or any Sub-contractor will use to Handle, or support the Handling of, Government Data and provide, manage 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.

3. Introduction

This Schedule sets out:

- 3.1 the Buyer's decision on where the Supplier may:
 - 3.1.1 store, access or Handle Government Data;
 - 3.1.2 undertake the Development Activity;
 - 3.1.3 host the Development Environment; and
 - 3.1.4 locate Support Locations,(in Paragraph 1);
- 3.2 the principles of security that apply to the Contract (in Paragraph 4);
- 3.3 the requirement to obtain a Risk Management Approval Statement (in Paragraphs 6 and 15);
- 3.4 the annual confirmation of compliance to be provided by the Supplier (in Paragraph 7);
- 3.5 the governance arrangements for security matters, where these are not otherwise specified in Call-Off Schedule 15 (*Call-Off Contract Management*) (in Paragraph 8);
- 3.6 access to staff (in Paragraph 9);

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

- 3.7 obligations in relation to Sub-contractors (in Paragraph 10);
- 3.8 the responsibility of the Buyer to determine the Supplier Information Management System that will be subject to Buyer-led Assurance (in Paragraph 11);
- 3.9 the Certification Requirements (in Paragraph 13);
- 3.10 the development, monitoring and updating of the Security Management Plan by the Supplier; or (in Paragraphs 14, 16 and 17);
- 3.11 the granting by the Buyer of approval for the Supplier to commence:
 - 3.11.1 the provision of Operational Services; and/or
 - 3.11.2 Handling Government Data (in Paragraph 15);
- 3.12 the management of changes to the Supplier Information Management System (in Paragraph 18); and
- 3.13 the Buyer's additional remedies for breach of this Schedule, including:
 - 3.13.1 the requirement for Remediation Action Plans (in Paragraph 19);
 - 3.13.2 the appointment of Independent Security Advisers (in Paragraph 20); and
 - 3.13.3 the withholding of Charges by the Buyer (in Paragraph 21).

4. Principles of security

- 4.1 The Supplier acknowledges that the Buyer places great emphasis on the confidentiality, integrity and availability of the Government Data and, consequently, on the security of:
 - 4.1.1 the Buyer System;
 - 4.1.2 the Supplier System;
 - 4.1.3 the Sites;
 - 4.1.4 the Services; and
 - 4.1.5 the Supplier Information Management System.
- 4.2 The Parties shall share information and act in a co-operative manner at all times to further the principles of security in Paragraph 4.1.
- 4.3 Notwithstanding the involvement of the Buyer in the Buyer-led Assurance of the Supplier Information Management System, the Supplier remains responsible for:
 - 4.3.1 the security, confidentiality, integrity and availability of the Government Data when that Government Data is under the control of the Supplier or any of its Sub-contractors; and
 - 4.3.2 the security of the Supplier Information Management System.

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

5. Security requirements

- 5.1 The Supplier must, and must ensure that Sub-contractors, design, build and manage the Supplier Information Management System in accordance with the Security Management Plan.
- 5.2 The Supplier must, unless otherwise agreed in writing with the Buyer:
 - 5.2.1 comply with the security requirements in Appendix 1;
 - 5.2.2 where the relevant option in Paragraph 1 is selected, comply with the security requirements for Development Activity in Appendix 2;
 - 5.2.3 where the relevant option in Paragraph 1 is selected, comply with the Buyer Security Policies; and
 - 5.2.4 ensure that Sub-contractors comply with:
 - (a) all security requirements in Appendix 1;
 - (b) where the relevant option in Paragraph 1 is selected, all security requirements for Development Activity in Appendix 2; and
 - (c) where the relevant option in Paragraph 1 is selected, all Buyer Security Policies,that apply to the activities that the Sub-contractor performs under its Sub-contract, unless:
 - (d) Paragraph 5.4 applies; or
 - (e) the table in Appendix 4 limits the security requirements in Appendix 1 or the security requirements for Development Activity in Appendix 2 that apply to a Sub-contractor.
- 5.3 Where the Buyer selects the option in Paragraph 1 requiring the Supplier to comply with the Buyer Security Policies, if there is an inconsistency between the Buyer Security Policies and the requirement of this Schedule, then the requirements of this Schedule will prevail to the extent of that inconsistency.
- 5.4 Where a Sub-contractor is a SMP Sub-contractor, the Supplier shall:
 - 5.4.1 use reasonable endeavours to ensure that the SMP Sub-contractor complies with all obligations that this Schedule imposes on Sub-contractors, including the security requirements in Appendix 1;
 - 5.4.2 document the differences between those obligations and the obligations that the SMP Sub-contractor is prepared to accept in sufficient detail to allow the Buyer to form an informed view of the risks concerned;
 - 5.4.3 take such steps as the Buyer may require to mitigate those risks.

6. Buyer to proceed

Notwithstanding anything in the Contract, the Supplier may not:

- 6.1 commence the provision of any Services; or

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

- 6.2 Handle any Government Data using the Supplier Information Management System,
unless
- 6.3 the Supplier has, and ensured that Sub-contractors have, obtained the Relevant Certifications under Paragraph 13;
- 6.4 the Supplier has completed an IT Health Check in accordance with Paragraph 12 of Appendix 1; and
- 6.5 the Buyer has issued a Risk Management Approval Statement under Paragraph 15.7.1.

7. Supplier confirmation

- 7.1 The Supplier must, no later than the last day of each Contract Year, provide to the Buyer a letter from its chief executive 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 the Contract;
 - 7.1.2 subject to Paragraph 7.2:
 - (a) it has fully complied with all requirements of this Schedule; and
 - (b) all Sub-contractors have complied with the requirements of this Schedule with which the Supplier is required to ensure they comply;
 - 7.1.3 the Supplier considers that its security and risk mitigation procedures remain effective.
- 7.2 Where the Buyer has, in respect of the period covered by the confirmation provided under Paragraph 7.1 agreed in writing that the Supplier need not, or need only partially, comply within any requirement of this Schedule:
 - 7.2.1 the confirmation must include details of the Buyer's agreement; and
 - 7.2.2 confirm that the Supplier has fully complied with that modified requirement.
- 7.3 The Supplier must:
 - 7.3.1 keep and maintain a register setting out all agreements referred to in Paragraph 7.2; and
 - 7.3.2 provide a copy of that register to the Buyer on request.

8. Governance, information sharing and co-operation

Governance

- 8.1 8.18.7The Buyer must establish a Security Working Group on which both the Buyer and the Supplier are represented.

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

- 8.2 The notice or other document establishing the Security Working Group must set out:
 - 8.2.1 the Buyer members;
 - 8.2.2 the Supplier members;
 - 8.2.3 the chairperson of the Security Working Group;
 - 8.2.4 the date of the first meeting;
 - 8.2.5 the frequency of meetings; and
 - 8.2.6 the location of meetings
- 8.3 The Security Working Group has oversight of all matters relating to the security of the Government Data and the Supplier Information Management System.
- 8.4 The Security Working Group meets:
 - 8.4.1 at least once every three months; and
 - 8.4.2 additionally when required by the Buyer.
- 8.5 The Supplier must ensure that the Supplier Staff attending each meeting of the Security Working Group:
 - 8.5.1 have sufficient knowledge and experience to contribute to the discussion of the matters on the agenda for the meeting;
 - 8.5.2 are authorised to make decisions that are binding on the Supplier in respect of those matters, including any decisions that require expenditure or investment by the Supplier; and
 - 8.5.3 where relevant to the matters on the agenda for the meeting, include representatives of relevant Sub-contractors.
- 8.6 Any decisions, recommendations or advice of the Security Working Group:
 - 8.6.1 are binding on the Supplier, unless
 - (a) the Buyer agrees otherwise; or
 - (b) the decision, recommendation or advice of the Security Working Group imposes on the Supplier more onerous requirements than those provided for in this Schedule; and
 - 8.6.2 do not limit or modify the Supplier's responsibilities under this Schedule.
- 8.7 Appendix 3 applies to the Security Working Group.
- 9. Staff**
- 9.1 The Supplier must ensure that at all times it maintains within the Supplier Staff sufficient numbers of qualified, skilled security professionals to ensure the Supplier complies with the requirements of this Schedule.
- 9.2 The Supplier must appoint:

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

- 9.2.1 a senior individual within its organisation with accountability for managing security risks and the Supplier's implementation of the requirements of this Schedule; and
- 9.2.2 a senior individual within the team responsible for the delivery of the Services with responsibility for managing the security risks to the Supplier Information Management System.
- 9.3 The individuals appointed under Paragraph 9.2:
 - 9.3.1 must have sufficient experience, knowledge and authority to undertake their roles effectively; and
 - 9.3.2 are to be designated as Key Staff and treated for the purposes of the Contract as Key Staff, whether or not they are otherwise designated as such;
- 9.4 The Supplier must review, and if necessary replace, the individuals appointed under Paragraph 9.2 if required to do so by the Buyer.
- 9.5 To facilitate:
 - 9.5.1 the Buyer-led Assurance and oversight of the Supplier Information Management System; and
 - 9.5.2 the Supplier's design, implementation, operation, management and continual improvement of the Security Management Plan and the security of the Services and Supplier Information Management System and otherwise,at reasonable times and on reasonable notice:
 - 9.5.3 the Supplier shall provide access to the Supplier Staff responsible for information assurance; and
 - 9.5.4 the Buyer shall provide access to its staff responsible for information assurance.

10. Sub-contractors

- 10.1 Paragraphs 10.2 to 10.4 are subject to Paragraph 5.4.

SIMS Sub-contractor

- 10.2 A SIMS Sub-contractor shall be treated for all purposes as a Key Subcontractor.
- 10.3 In addition to the obligations imposed by the Contract on Key Subcontractors, the Supplier must ensure that the Key Sub-Contract with each SIMS Sub-contractor:
 - 10.3.1 contains obligations no less onerous on the Key Subcontractor than those imposed on the Supplier under this Schedule; and
 - 10.3.2 provides for the Buyer to perform Buyer-led Assurance of any part of the Supplier Information Management System that the SIMS Sub-

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

contractor provides or operates that is not otherwise subject to Buyer-led Assurance under this Schedule.

Sub-contractors

- 10.4 The Supplier must, before entering into a binding Sub-contract with any Sub-contractor:
 - 10.4.1 undertake sufficient due diligence of the proposed Sub-contractor to provide reasonable assurance that the proposed Sub-contractor can perform the obligations that this Schedule requires the Supplier ensure that the proposed Sub-contractor performs;
 - 10.4.2 keeps adequate records of the due diligence it has undertaken in respect of the proposed Sub-contractors; and
 - 10.4.3 provides those records to the Buyer on request.

Key Subcontractor Default

- 10.5 Where the Supplier becomes aware of an actual or suspected failure by a Key Subcontractor to comply with any obligation in this Schedule with which the Supplier is, by virtue of Paragraph 5.2.45.2.2, required to ensure the Key Subcontractor complies (**Key Sub-contractor Default**), the Supplier must:
 - 10.5.1 as soon as reasonably practicable and in any event within two Working days of becoming aware of the Key Subcontractor Default notify the Buyer setting out the actual or anticipated effect of the Key Subcontractor Default; and
 - 10.5.2 unless the Buyer waives the requirement, comply with the Remediation Action Plan process in Paragraph 19.

11. Supplier Information Management System

- 11.1 The Buyer must determine:
 - 11.1.1 the scope and component parts of the Supplier Information Management System; and
 - 11.1.2 the boundary between the Supplier Information Management System and the Wider Information Management System.
- 11.2 To enable the Buyer to make that determination, the Supplier shall provide the Buyer with such documentation and information that the Buyer may require regarding the Wider Information Management System.
- 11.3 The Buyer shall notify the Supplier, as soon as reasonably practical, following the receipt of such documentation and information, of its decision regarding:
 - 11.3.1 the scope and component parts of the Supplier Information Management System;
 - 11.3.2 its boundary with the Wider Information Management System.
- 11.4 Before reaching its decision under Paragraph 11.3, the Buyer must consult with the Supplier concerning its proposed decision.

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

- 11.5 The Supplier shall reproduce the Buyer's decision as a diagram documenting the components and systems forming part of, and the boundary between, the Supplier Information Management System and the Wider Information Management System.
- 11.6 The diagram prepared under Paragraph 11.5 forms part of the Security Management Plan.
- 11.7 Any proposed change to:
 - 11.7.1 the component parts of the Supplier Information Management System;
or
 - 11.7.2 the boundary between the Supplier Information Management System and the Wider Information Management System,
is:
 - 11.7.3 an Variation to which the Variation Procedure applies;
 - 11.7.4 requires approval by the Buyer under Paragraph 18; and
 - 11.7.5 the Buyer may require the appointment of an Independent Security Adviser to advise on the proposed change.
- 12. Government Data Handled using Supplier Information Management System**
 - 12.1 The Supplier acknowledges that the Supplier Information Management System:
 - 12.1.1 is intended only for the Handling of Government Data that is classified as OFFICIAL; and
 - 12.1.2 is not intended for the Handling of Government Data that is classified as SECRET or TOP SECRET,
in each case using the Government Security Classification Policy.
 - 12.2 The Supplier must:
 - 12.2.1 not alter the classification of any Government Data; and
 - 12.2.2 if it becomes aware that any Government Data classified as SECRET or TOP SECRET is being Handled using the Supplier Information Management System:
 - (a) immediately inform the Buyer; and
 - (b) follow any instructions from the Buyer concerning that Government Data.
 - 12.3 The Supplier must, and must ensure that Sub-contractors and Supplier Staff, when Handling Government Data, comply with:
 - 12.3.1 the Expected Behaviours; and
 - 12.3.2 the Security Controls.

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

- 12.4 Where there is a conflict between the Expected Behaviours or the Security Controls and this Schedule the provisions of this Schedule shall apply to the extent of any conflict.

13. Certification Requirements

- 13.1 The Supplier shall ensure that, unless otherwise agreed by the Buyer, both:

13.1.1 it; and

13.1.2 any SIMS Sub-contractor, any Key Subcontractor, any Higher-risk Sub-contractor and any Medium-risk Sub-contractor,

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

13.1.3 in the case of the Supplier, any SIMS Sub-contractor and any Key Subcontractor:

(a) either:

(i) an ISO Certification in respect of the Supplier Information Management System; or

(ii) where the Supplier Information Management System is included within the scope of a wider ISO Certification, that ISO Certification; and

(b) Cyber Essentials Plus;

(or equivalent); and

13.1.4 In the case of any Higher-risk Sub-contractor, either:

(a) an ISO Certification in respect of that part of the Supplier Information Management System provided by the Higher-risk Sub-contractor;

(b) where that part of the Supplier Information Management System provided by the Higher-risk Sub-contractor is included within the scope of a wider ISO Certification, that ISO Certification; or

(c) Cyber Essentials Plus; and

13.1.5 in the case of any Medium-risk Sub-contractor, Cyber Essentials (or equivalent).

- 13.2 Unless otherwise agreed by the Buyer, before it begins to provide the Services, the Supplier must provide the Buyer with a copy of:

13.2.1 the Relevant Certifications for it and any Sub-contractor; and

13.2.2 the relevant scope and statement of applicability required under the ISO/IEC 27001 Relevant Certifications.

- 13.3 The Supplier must ensure that at the time it begins to provide the Services, the Relevant Certifications for it and any Sub-contractor are:

13.3.1 currently in effect;

13.3.2 together, cover at least the full scope of the Supplier Information Management System; and

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

- 13.3.3 are not subject to any condition that may impact the provision of the Services or the Development Activity (**Certification Requirements**).
- 13.4 The Supplier must notify the Buyer promptly, and in any event within three Working Days, after becoming aware that, in respect of it or any Sub-contractor:
 - 13.4.1 a Relevant Certification in respect of the Supplier Information Management System has been revoked or cancelled by the body that awarded it;
 - 13.4.2 a Relevant Certification in respect of the Supplier Information Management System has expired and has not been renewed by the Supplier;
 - 13.4.3 the Relevant Certifications, together, no longer apply to the full scope of the Supplier Information Management System; or
 - 13.4.4 the body that awarded a Relevant Certification has made it subject to conditions, the compliance with which may impact the provision of the Services (each a **Certification Default**)
- 13.5 Where the Supplier has notified the Buyer of a Certification Default under Paragraph 13.4:
 - 13.5.1 the Supplier must, within ten Working Days of the date in which the Supplier provided notice under Paragraph 13.4 (or such other period as the Parties may agree) provide a draft plan (**Certification Rectification Plan**) to the Buyer setting out:
 - (a) full details of the Certification Default, including a root cause analysis;
 - (b) the actual and anticipated effects of the Certification Default;
 - (c) the steps the Supplier and any Sub-contractor to which the Certification Default relates will take to remedy the Certification Default;
 - 13.5.2 the Buyer must notify the Supplier as soon as reasonably practicable whether it accepts or rejects the Certification Rectification Plan;
 - 13.5.3 if the Buyer rejects the Certification Rectification Plan, the Supplier must within five Working Days of the date of the rejection submit a revised Certification Rectification Plan and Paragraph 13.5.2 will apply to the re-submitted plan;
 - 13.5.4 the rejection by the Buyer of a revised Certification Rectification Plan is a material Default of the Contract;
 - 13.5.5 if the Buyer accepts the Certification Rectification Plan, the Supplier must start work immediately on the plan.

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

14. Security Management Plan

Purpose of Security Management Plan

- 14.1 The Buyer may, at any time, provide the Supplier with a Statement of Information Risk Appetite.
- 14.2 The Supplier must document in the Security Management Plan how the Supplier and its Sub-contractors will:
 - 14.2.1 comply with the requirements set out in this Schedule and the Contract in order to ensure the security of the Government Data and the Supplier Information Management System; and
 - 14.2.2 ensure that the operation of the Supplier Information Management System and the provision of the Services does not give rise to any information security risks greater than those set out in that Statement of Information Risk Appetite (where one has been provided).
- 14.3 The Supplier must ensure that:
 - 14.3.1 the Security Management Plan accurately represents the Supplier Information Management System;
 - 14.3.2 the Supplier Information Management System will meet the requirements of this Schedule and the Statement of Information Risk Appetite (where one has been provided); and
 - 14.3.3 the residual risks of the Supplier Information Management System are no greater than those provided for in the Statement of Information Risk Appetite (where one has been provided).

Preparation of Security Management Plan

- 14.4 The Supplier must prepare and submit the Security Management Plan to the Buyer:
 - 14.4.1 by the date specified in the Detailed Implementation Plan; or
 - 14.4.2 if no such date is specified, in sufficient time to allow for the Buyer to:
 - (a) approve the Security Management Plan; and
 - (b) undertake any Buyer-led Assurance activity, before the Start Date.
- 14.5 If Paragraph 14.4.2 applies, and any delay resulting from the Buyer-led Assurance causes or contributes to Supplier Non-Performance that delay is not an Authority Cause and the Supplier shall not be entitled to any relief or compensation under Clause 5.1 (*The Buyer's obligations to the Supplier*) of the General Terms.

Contents of Security Management Plan

- 14.6 The Security Management Plan must include:
 - 14.6.1 a formal information risk assessment of, and a risk treatment plan for, the Supplier Information Management System;

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

- 14.6.2 a completed statement of applicability under the relevant ISO Certification for the Supplier Information Management System;
- 14.6.3 the process for managing any security risks from Sub-contractors and third parties with access to the Services, the Supplier Information Management System or the Government Data;
- 14.6.4 unless the Buyer has waived such requirement by selecting the relevant option in Paragraph 1, an assessment of the Supplier Information Management System against the table in Appendix 5 (Secure by Design Principles Evaluation Table);
- 14.6.5 unless such requirement is waived by the Buyer, the controls the Supplier will implement in respect of the Services and all processes associated with the delivery of the Services, including:
 - (a) the Supplier System;
 - (b) the Sites; and
 - (c) the Buyer System (to the extent that it is under the control of the Supplier); and
 - (d) any IT, Information and data (including the Confidential Information of the Buyer and the Government Data) to the extent used by the Buyer or the Supplier:
 - (i) in connection with the Contract or
 - (ii) in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Services;
- 14.6.6 the Required Changes Register;
- 14.6.7 evidence that the Supplier and each Sub-contractor (so far as those requirements apply) is compliant with:
 - (a) the Certification Requirements;
 - (b) the security requirements in Appendix 1; and
 - (c) where the relevant option in Paragraph 1 is selected, the security requirements for Development Activity in Appendix 2;
- 14.6.8 the diagram documenting the Supplier Information Management System, the Wider Information Management System and the boundary between them (created under Paragraph 11).
- 14.6.9 an assessment of the Supplier Information Management System against the requirements of this Schedule, including the security requirements in Appendix 1 and, where the relevant option in Paragraph 1 is selected, the security requirements for Development Activity in Appendix 2 (where applicable);
- 14.6.10 the process the Supplier will implement immediately after it becomes aware of a Breach of Security to restore normal operations as

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

quickly as possible, minimising any adverse impact on the Government Data, the Buyer, the Services and/or users of the Services; and

- 14.6.11 the following information, so far as is applicable, in respect of each Sub-contractor:
- (a) the Sub-contractor's:
 - (i) legal name;
 - (ii) trading name (if any); and
 - (iii) registration details (where the Sub-contractor is not an individual);
 - (b) the Relevant Certifications held by the Sub-contractor;
 - (c) the Sites used by the Sub-contractor;
 - (d) the Services provided, or contributed to, by the Sub-contractor;
 - (e) the access the Sub-contractor has to the Supplier Information Management System;
 - (f) the Government Data Handled by the Sub-contractor;
 - (g) the Handling that the Sub-contractor will undertake in respect of the Government Data; and
 - (h) the measures the Sub-contractor has in place to comply with the requirements of this Schedule; and
 - (i) the due diligence the Supplier has taken to assess that compliance;
- 14.6.12 the Register of Sites, Support Locations and Third-party Tools;
- 14.6.13 the Modules Register;
- 14.6.14 the Support Register;
- 14.6.15 the Backup and Recovery Plan;
- 14.6.16 the Remote Working Policy (where the Supplier or a Sub-contractor proposes to allow Supplier Staff to work from a Remote Location); and
- 14.6.17 details of the protective monitoring that the Supplier will undertake in accordance with Paragraph 14 of Appendix 1, including:
- (a) the additional audit and monitoring the Supplier will undertake of the Supplier Information Management System; and
 - (b) the retention periods for audit records and event logs.

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

15. Buyer-led Assurance of Supplier Information Management System

- 15.1 The Buyer will undertake Buyer-led Assurance of the Supplier Information Management System in accordance with this Paragraph 15.
- 15.2 The Supplier acknowledges that the purpose of Buyer-led Assurance is to ensure that:
 - 15.2.1 the Security Management Plan accurately represents the Supplier Information Management System;
 - 15.2.2 the Buyer has sufficient confidence that the Supplier Information Management System will meet the requirements of this Schedule and the Statement of Information Risk Appetite (where one has been provided); and
 - 15.2.3 the residual risks of the Supplier Information Management System are no greater than those provided for in the Statement of Information Risk Appetite (where one has been provided).
- 15.3 The Buyer, or representatives appointed by the Buyer, will perform Buyer-led Assurance.
- 15.4 In addition to any obligations imposed by Call-Off Schedule 13 (*Implementation Plan and Testing*) the Supplier must ensure that its Implementation Plan includes:
 - 15.4.1 sufficient information concerning the steps it will take to ensure compliance with the requirements of this Schedule, including any requirements imposed on Sub-contractors;
 - 15.4.2 provision for sufficient time for the Buyer to undertake any Buyer-led Assurance activities;
 - 15.4.3 provision for sufficient time for the Supplier to address any issued raised by the Buyer should it issue a Risk Management Rejection Notice.
- 15.5 In particular, the Detailed Implementation Plan must include:
 - 15.5.1 the dates on which each subsequent iteration of the Security Management Plan will be delivered to the Buyer for review and staged approval; and
 - 15.5.2 the date by which the Supplier is required to have received a Residual Risk Statement from the Buyer together with details of each:
 - (a) tasks the Supplier must complete, including any required Security Tests;
 - (b) Milestones which must be Achieved; and
 - (c) Buyer Responsibilities which must be completedfor the Supplier to receive a Risk Management Approval Statement pursuant to Paragraph 15.7.1;

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

15.6 To facilitate Buyer-led Assurance of the Supplier Information Management System, the Supplier shall provide the Buyer and its authorised representatives with:

15.6.1 such access as the Buyer or its authorised representative requires to the Supplier Information Management System; and

15.6.2 such other information and/or documentation that the Buyer or its authorised representatives may require.

15.7 The Buyer shall, by the relevant date set out in the Detailed Implementation Plan, review the Security Management Plan and undertake such further investigations as it considers necessary or desirable, and issue to the Supplier:

15.7.1 where satisfied that the:

(a) identified risks to the Supplier Information Management System are adequately and appropriately addressed; and

(b) that the residual risks are:

(i) either:

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

(2) where the Buyer has not provided a Statement of Information Risk Appetite, reduced to an acceptable level;

(ii) understood and accepted by the Buyer; and

(iii) recorded in the Residual Risk Statement;

a Risk Management Approval Statement; or

15.7.2 where the Buyer reasonably considers that:

(a) the identified risks to the Supplier Information Management System have not been adequately or appropriately addressed; or

(b) the residual risks to the Supplier Information Management System have not been reduced:

(i) where the Buyer has Provided a Statement of Information Risk Appetite, to the level anticipated by that statement; or

(ii) where the Buyer has not Provided a Statement of Information Risk Appetite, to an acceptable level,

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

15.8 When issued, the Risk Management Approval Statement forms part of the Security Management Plan.

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

- 15.9 If the Buyer issues a Risk Management Rejection Notice, the Supplier shall, within [20] Working Days of the date of the Risk Management Rejection Notice:
- 15.9.1 address all of the issues raised by the Buyer;
 - 15.9.2 update the Security Management Plan; and
 - 15.9.3 notify the Buyer that the Supplier Information Management System is ready for re-assessment under Paragraph 15.7.
- 15.10 The process set out in Paragraphs 15.7 to 15.9 shall be repeated until such time as the Buyer issues a Risk Management Approval Statement to the Supplier or terminates the Contract.
- 15.11 The Supplier shall not use the Supplier Information Management System to Handle Government Data before receiving a Risk Management Approval Statement.
- 15.12 The Supplier is solely responsible for the costs of:
- 15.12.1 developing and updating the Security Management Plan; and
 - 15.12.2 implementing changes to the Supplier Information Management System required by any Risk Management Rejection Notice.

16. Monitoring and updating Security Management Plan

Updating Security Management Plan

- 16.1 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

- 16.2 The Supplier, where it plans to undertake, or after becoming aware of, any of the following:
- 16.2.1 a significant change to the components or architecture of the Supplier Information Management System;
 - 16.2.2 a significant change in the boundary between the Supplier Information Management System and the Wider Information Management System
 - 16.2.3 a significant change in the operation of the Supplier Information Management System;
 - 16.2.4 the replacement of an existing, or the appointment of a new:
 - (a) SIMS Sub-contractor; or
 - (b) Sub-contractor that Handles Government Data;
 - 16.2.5 a significant change in the quantity of Personal Data held within the Service; and/or
 - 16.2.6 where the Supplier or a Sub-contractor has previously Handled Government Data that is Personal Data, other than Special Category

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

Personal Data, it proposes to start to Handle Government Data that is Special Category Personal Data under the Contract;

must:

16.2.7 within two Working Days notify the Buyer; and

16.2.8 within ten Working Days, or such other timescale as may be agreed with the Buyer:

- (a) update the Required Changes Register and any other affected parts of the Security Management Plan; and
- (b) provide the Buyer with a copy those documents for review and approval.

16.3 Paragraph 16.2 applies in addition to, and not in substitution of, the Parties obligations to comply with the Variation Procedure for any Variation.

16.4 Any proposed change under Paragraph 16.2.1, 16.2.2 or 16.2.6 constitutes a Variation to which the Variation Procedure applies.

17. Review and approval of updated Security Management Plan

17.1 Where the Supplier has updated the Security Management Plan under Paragraph 16, the Buyer may review the updated plans, require the provision of such further information, and undertake such further investigations as the Buyer considers necessary or desirable.

17.2 At the conclusion of that review, it may issue to the Supplier:

17.2.1 where satisfied that the:

- (a) identified risks to the Supplier Information Management System are adequately and appropriately addressed; and
- (b) that the residual risks are:
 - (i) either:
 - (1) where the Buyer has provided a Statement of Information Risk Appetite, reduced to the level anticipated by that statement; or
 - (2) where the Buyer has not provided a Statement of Information Risk Appetite, reduced to an acceptable level;
 - (ii) understood and accepted by the Buyer; and
 - (iii) recorded in the Residual Risk Statement;

a Risk Management Approval Statement; or

17.2.2 where the Buyer considers that:

- (a) the identified risks to the Supplier Information Management System have not been adequately or appropriately addressed; or

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

- (b) the residual risks to the Supplier Information Management System have not been reduced:
 - (i) where the Buyer has Provided a Statement of Information Risk Appetite, to the level anticipated by that statement; or
 - (ii) where the Buyer has not Provided a Statement of Information Risk Appetite, to an acceptable level,
- a Risk Management Rejection Notice, with the reasons for its decision.

18. Changes to the Supplier Information Management System

18.1 Notwithstanding anything in the Contract, the Supplier must obtain the approval of the Buyer before making any of the following changes to the Supplier Information Management System:

18.1.1 a significant change in the systems or components making up the Supplier Information Management System;

18.1.2 a significant change in the operation or management of the Supplier Information Management System; or

18.1.3 the appointment of a new, or the replacement of an existing:

- (a) SIMS Sub-contractor; or
- (b) Sub-contractor that Handles Government Data.

18.2 In seeking the Buyer's approval to a proposed changes to the Supplier Information Management System, the Supplier must:

18.2.1 update the Required Changes Register;

18.2.2 prepare a proposal for the Buyer setting out:

- (a) details of the proposed changes to the Supplier Information Management System;
- (b) an assessment of the security implications of the proposed change;
- (c) a risk assessment of the proposed change; and
- (d) any proposed changes to the Security Management Plan; and

18.2.3 provide that paper to the Buyer no later than 30 Working Days before the date on which it will consider the proposed changes.

18.3 The Buyer:

18.3.1 may request such further information as the Buyer considers necessary or desirable;

18.3.2 must provide its decision within 20 Working Days of the later of:

- (a) the date on which it receives the proposal; or
- (b) the date on which it receives any requested further information;

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

18.3.3 must not:

- (a) unreasonably refuse any proposal by the Supplier; and
- (b) must not make any approval subject to unreasonable conditions.

18.4 If the Buyer does not provide a decision within the period specified in Paragraph 18.3.2, the proposal shall be deemed to have been accepted.

Implementation of changes

18.5 Where the Supplier implements a necessary change to the Supplier Information Management System to address a security related risk or vulnerability, the Supplier shall effect such change at its own cost and expense.

18.6 If the Supplier does not implement a necessary change to the Supplier Information Management System to address a security related risk or vulnerability by the date set out in the Required Changes Register:

18.6.1 that failure is a material Default; and

18.6.2 the Supplier shall:

- (a) immediately cease using the Supplier Information Management System to Handle Government Data either:
 - (i) until the Default is remedied, or
 - (ii) unless directed otherwise by the Buyer in writing and then only in accordance with the Buyer's written directions; and
- (b) where such material Default is capable of remedy, remedy such material Default within the timescales set by the Buyer (considering the security risks the material Default presents to the Services and/or the Supplier Information Management System).

19. Remediation Action Plan

Preparation of Remediation Action Plan

19.1 This Paragraph 19 applies when:

19.1.1 Key Subcontractor Default occurs;

19.1.2 the Buyer issues a Risk Management Rejection Notice; or

19.1.3 the Supplier receives a Security Test report identifies vulnerabilities in, or makes findings in respect of, the Supplier Information Management System,

(each a **RAP Trigger**).

19.2 The Supplier must within [20] Working Days of the occurrence of a RAP Trigger prepare and submit for approval to the Buyer a draft plan (**Remediation Action Plan**).

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

- 19.3 The draft Remediation Action Plan must, in respect of each issue raised by the RAP Trigger, set out:
- 19.3.1 full details of that issue;
 - 19.3.2 the actual or anticipated effect of that issue;
 - 19.3.3 how the issue will be remedied;
 - 19.3.4 the date by which the issue will be remedied; and
 - 19.3.5 the tests that the Supplier proposes to perform to confirm that the issue has been remedied.

Consideration of Remediation Action Plan

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

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

Implementing an approved Remediation Action Plan

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

20. Independent Security Adviser

- 20.1 The Buyer may require the appointment of an Independent Security Adviser where:
- 20.1.1 there is a proposed change to the Supplier Information Management System (see Paragraph 11.7);
- 20.1.2 the Buyer issues two or more Risk Management Rejection Notices (see Paragraphs 15.7 and 15.10; or
- 20.1.3 either:
- (a) a Security Test report identifies more than ten vulnerabilities classified as either critical or high; or
 - (b) the Buyer rejected a revised draft Remediation Action Plan (see Paragraph 12.21 of Appendix 1).
- 20.2 Where the Buyer requires the appointment of an Independent Security Adviser, the Independent Security Adviser shall be:
- 20.2.1 a person selected by the Supplier and approved by the Buyer; or
- 20.2.2 where
- (a) the Buyer does not approve the persons selected by the Supplier; or
 - (b) the Supplier does not select any person within ten Working Days of the date of the notice requiring the Independent Security Adviser's appointment,

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

a person selected by the Buyer.

20.3 The terms of the Independent Security Adviser's appointment shall require that person to:

20.3.1 undertake a detailed review, including a full root cause analysis where the Independent Security Adviser considers it appropriate to do so, of the circumstances that led to that person's appointment; and

20.3.2 provide advice and recommendations on:

- (a) steps the Supplier can reasonably take to improvement the security of the Supplier Information Management System; and
- (b) where relevant, how the Supplier may mitigate the effects of, and remedy, those and to avoid the occurrence of similar circumstances to those leading to the appointment of the Independent Security Adviser in the future.

20.4 The Supplier must permit, and must ensure that relevant Sub-contractors permit, the Independent Security Adviser to:

20.4.1 observe the conduct of and work alongside the Supplier Staff to the extent that the Independent Security Adviser considers reasonable and proportionate having regard to reason for their appointment;

20.4.2 gather any information the Independent Security Adviser considers relevant in the furtherance of their appointment;

20.4.3 write reports and provide information to the Buyer in connection with the steps being taken by the Supplier to remedy the matters leading to the Independent Security Adviser's appointment;

20.4.4 make recommendations to the Buyer and/or the Supplier as to how the matters leading to their appointment might be mitigated or avoided in the future; and/or

20.4.5 take any other steps that the Buyer and/or the Independent Security Adviser reasonably considers necessary or expedient in order to mitigate or rectify matters leading to the Independent Security Adviser's appointment.

20.5 The Supplier must, and ensure that relevant Sub-contractors:

20.5.1 where relevant, work alongside, provide information to, co-operate in good faith with and adopt any reasonable methodology in providing the Services recommended by the Independent Security Adviser in order to mitigate or rectify any of the vulnerabilities that led to the appointment of the Independent Security Adviser;

20.5.2 ensure that the Independent Security Adviser has all the access it may require in order to carry out its objective, including access to the Assets;

20.5.3 submit to such monitoring as the Buyer and/or the Independent Security Adviser considers reasonable and proportionate in respect of the matters giving rise to their appointment;

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

- 20.5.4 implement any recommendations (including additional security measures and/or controls) made by the Independent Security Adviser that have been approved by the Buyer within the timescales given by the Independent Security Adviser; and
- 20.5.5 not terminate the appointment of the Independent Security Adviser without the prior consent of the Buyer (unless such consent has been unreasonably withheld).
- 20.6 The Supplier shall be responsible for:
 - 20.6.1 the costs of appointing, and the fees charged by, the Independent Security Adviser; and
 - 20.6.2 its own costs in connection with any action required by the Buyer and/or the Independent Security Adviser.
- 20.7 If the Supplier or any relevant Sub-contractor:
 - 20.7.1 fails to perform any of the steps required by the Buyer in the notice appointing the Independent Security Adviser; and/or
 - 20.7.2 is in Default of any of its obligations under this Paragraph 20, this is a material Default that is not capable of remedy.
- 21. Withholding of Charges**
 - 21.1 The Buyer may withhold some or all of the Charges in accordance with the provisions of this Paragraph 21 where:
 - 21.1.1 the Supplier is in material Default of any of its obligations under this Schedule; or
 - 21.1.2 any of the following matters occurs (where those matters arise from a Default by the Supplier of its obligations under this Schedule):
 - (a) a Notifiable Default;
 - (b) an Intervention Cause; or
 - (c) a Step-in Trigger Event.
 - 21.2 The Buyer may withhold an amount of the Charges that it considers sufficient, in its sole discretion, to incentivise the Supplier to perform the obligations it has Defaulted upon.
 - 21.3 Before withholding any Charges under Paragraph 21.1 the Buyer must
 - 21.3.1 provide written notice to the Supplier setting out:
 - (a) the Default in respect of which the Buyer has decided to withhold some or all of the Charges;
 - (b) the amount of the Charges that the Buyer will withhold;
 - (c) the steps the Supplier must take to remedy the Default;
 - (d) the date by which the Supplier must remedy the Default;

Call-Off Schedule 9E (Security: Buyer-led Assurance)

Call-Off Ref:

Crown Copyright 2025

- (e) the invoice in respect of which the Buyer will withhold the Charges; and
- 21.3.2 consider any representations that the Supplier may make concerning the Buyer's decision.
- 21.4 Where the Supplier does not remedy the Default by the date specified in the notice given under Paragraph 21.3.1, the Buyer may retain the withheld amount.
- 21.5 The Supplier acknowledges:
 - 21.5.1 the legitimate interest that the Buyer has in ensuring the security of the Supplier Information Management System and the Government Data and, as a consequence, the performance by the Supplier of its obligations under this Schedule; and
 - 21.5.2 that any Charges that are retained by the Buyer are not out of all proportion to the Buyer's legitimate interest, even where:
 - (a) the Buyer has not suffered any Losses as a result of the Supplier's Default; or
 - (b) the value of the Losses suffered by the Buyer as a result of the Supplier's Default is lower than the amount of the Charges retained.
- 21.6 The Supplier may raise a Dispute under the Dispute Resolution Procedure with any decision by the Buyer to:
 - 21.6.1 withhold any Charges under Paragraph 21.1; or
 - 21.6.2 retain any Charges under Paragraph 21.4.
- 21.7 Any Dispute raised by the Supplier does not prevent the Buyer withholding Charges in respect of:
 - 21.7.1 the decision subject to the Dispute; or
 - 21.7.2 any other matter to which this Paragraph 21 applies.
- 21.8 Where any Dispute raised by the Supplier is resolved wholly or partially in its favour, the Buyer must return such sums as are specified in any agreement or other document setting out the resolution of the Dispute.
- 21.9 The Buyer's right to withhold or retain any amount under this Paragraph 21 are in addition to any other rights that the Buyer may have under the Contract or in Law, including any right to claim damages for Losses it suffers arising from the Default.

22. Access to Buyer System

- 22.1 Where the Supplier, a Sub-contractor or any of the Supplier Staff is granted access to the Buyer System or to the Buyer Equipment, it must comply with and ensure that all such Sub-contractors and Supplier Staff comply with, all rules, policies and guidance provided to it and as updated from time to time concerning the Buyer System or the Buyer Equipment.

Appendix 1 Security requirements

1 Location

Location for Relevant Activities

- 1.1 Unless otherwise agreed with the Buyer, the Supplier must, and ensure that its Sub-contractors, at all times:
 - 1.1.1 provide the Services;
 - 1.1.2 undertake any activity supporting or managing:
 - (a) the Services;
 - (b) the Supplier Information Management System; or
 - (c) the Wider Information Management System;
 - 1.1.3 store, access or Handle Government Data;
 - 1.1.4 undertake the Development Activity; and
 - 1.1.5 host the Wider Information Management System, including any Sites (together, the **Relevant Activities**)only in or from the geographic areas permitted by the Buyer in Paragraph 1.
- 1.2 Where the Buyer has not selected an option concerning location in Paragraph 1, the Supplier may only undertake the Relevant Activities in or from:
 - 1.2.1 the United Kingdom; or
 - 1.2.2 a territory permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State).
- 1.3 The Supplier must, and must ensure that its Sub-contractors, undertake the Relevant Activities in a facility operated by an entity where:
 - 1.3.1 the entity has entered into a binding agreement with the Supplier or Sub-contractor (as applicable);
 - 1.3.2 that binding agreement includes obligations on the entity in relation to security management equivalent to those imposed on Sub-contractors in this Schedule;
 - 1.3.3 the Supplier or Sub-contractor has taken reasonable steps to assure itself that the entity complies with the binding agreement;
 - 1.3.4 the Supplier has provided the Buyer with such information as the Buyer requires concerning:
 - (a) the entity;
 - (b) the arrangements with the entity; and
 - (c) the entity's compliance with the binding agreement; and

- 1.3.5 the Buyer has not given the Supplier a Prohibition Notice under Paragraph 1.11.
- 1.4 Where the Supplier cannot comply with one or more of the requirements of Paragraph 1.3:
 - 1.4.1 it must provide the Buyer with such information as the Buyer requests concerning:
 - (a) the security controls in places at the relevant location or locations; and
 - (b) where certain security controls are not, or only partially, implemented the reasons for this;
 - 1.4.2 the Buyer may grant approval to use that location or those locations, and that approval may include conditions; and
 - 1.4.3 if the Buyer does not grant permission to use that location or those locations, the Supplier must, within such period as the Buyer may specify:
 - (a) cease to store, access or Handle Government Data at that location or those locations;
 - (b) sanitise, in accordance with instructions from the Buyer, such equipment within the information and communications technology system used to store, access or Handle Government Data at that location, or those locations, as the Buyer may specify.

Support Locations

- 1.5 The Supplier must ensure that all Support Locations are located only in the geographic areas permitted by the Buyer.
- 1.6 Where the Buyer has not selected an option concerning location in Paragraph 1, the Supplier may only locate Support Locations in:
 - 1.6.1 the United Kingdom; or
 - 1.6.2 a territory permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State).
- 1.7 The Supplier must, and must ensure that its Sub-contractors operate the Support Locations in a facility operated by an entity where:
 - 1.7.1 the entity has entered into a binding agreement with the Supplier or Sub-contractor (as applicable);
 - 1.7.2 the binding agreement includes obligations on the entity in relation to security management equivalent to those relating to Sub-contractors in this Schedule;
 - 1.7.3 the Supplier or Sub-contractor has taken reasonable steps to assure itself that the entity complies with the binding agreement;

1.7.4 the Supplier has provided the Buyer with such information as the Buyer requires concerning:

- (a) the entity;
- (b) the arrangements with the entity; and
- (c) the entity's compliance with the binding agreement; and

1.7.5 the Buyer has not given the Supplier a Prohibition Notice under Paragraph 1.11.

Third-party Tools

1.8 Before using any Third-party Tool, the Supplier must, and must ensure that its Sub-contractors:

1.8.1 perform adequate due diligence to determine whether there are any recognised security vulnerabilities with that Third-party Tool;

1.8.2 the Supplier has provided the Buyer with such information as the Buyer requires concerning:

- (a) the arrangements with the provider of the Third-party Tool; and
- (b) the due diligence undertaken by the Supplier or Sub-contractor; and

1.8.3 do not use a Third-party Tool in respect of which the Buyer has given the Supplier a Prohibition Notice under Paragraph 1.11.

1.9 The Supplier must use, and ensure that Sub-contractors use, only those Third-party Tools included in the Register of Sites, Support Locations and Third-party Tools.

1.10 The Supplier must not, and must not allow Sub-contractors to, use:

1.10.1 a Third-party Tool other than for the activity specified for that Third-party Tool in the Register of Sites, Support Locations and Third-party Tools; or

1.10.2 a new Third-party Tool, or replace an existing Third-party Tool, without the permission of the Buyer.

Prohibited Activities

1.11 The Buyer may by notice in writing at any time give notice to the Supplier that it and its Sub-contractors must not:

1.11.1 undertake or permit to be undertaken some or all of the Relevant Activities or operate Support Locations (**Prohibited Activity**).

- (a) in any particular country or group of countries;
- (b) in or using facilities operated by any particular entity or group of entities; or
- (c) in or using any particular facility or group of facilities, whether operated by the Supplier, a Sub-contractor or a third -party entity; or

1.11.2 use any specified Third-party Tool,

(a **Prohibition Notice**).

1.12 Where the Supplier or Sub-contractor, on the date of the Prohibition Notice:

1.12.1 undertakes any Prohibited Activities;

1.12.2 operates any Support Locations; or

1.12.3 employs any Third-party Tool,

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

2 Physical Security

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

2.1.1 all Sites, locations at which Relevant Activities are performed, or Support Locations (**Secure Locations**) have the necessary physical protective security measures in place to prevent unauthorised access, damage and interference, whether malicious or otherwise, to Government Data;

2.1.2 the operator of the Secure Location has prepared a physical security risk assessment and a site security plan for the Secure Location; and

2.1.3 the physical security risk assessment and site security plan for each Secure Location:

- (a) considers whether different areas of the Secure Location require different security measures based on the functions of each area;
- (b) adopts a layered approach to physical security;
- (c) has sections dealing with the following matters:
 - (i) the perimeter of the Secure Location;
 - (ii) the building fabric;
 - (iii) security guarding;
 - (iv) visitor and people management;
 - (v) server and communications rooms;
 - (vi) protection of sensitive data;
 - (vii) closed circuit television;
 - (viii) automated access and control systems;
 - (ix) intruder detection; and
 - (x) security control rooms.

2.2 The Supplier must provide the Buyer with the physical security risk assessment and site security plan for any Secure Location within 20 Working Days of a request by the Buyer.

3 Vetting, Training and Staff Access

Vetting before performing or managing Services

- 3.1 The Supplier must not engage Supplier Staff, and must ensure that Sub-contractors do not engage Supplier Staff in:
 - 3.1.1 any activity relating to the provision or management of the Services; or
 - 3.1.2 any activity that allows or requires the Handling of Government Data, unless:
 - 3.1.3 that individual has passed the security checks listed in Paragraph 3.2; or
 - 3.1.4 the Buyer has given prior written permission for a named individual to perform a specific role.
- 3.2 For the purposes of Paragraph 3.1, the security checks are:
 - 3.2.1 The checks required for the HMG Baseline Personnel Security Standard (BPSS) to verify:
 - (a) the individual's identity;
 - (b) 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;
 - (c) the individual's previous employment history; and
 - (d) that the individual has no Relevant Convictions;
 - 3.2.2 national security vetting clearance to the level specified by the Buyer for such individuals or such roles as the Buyer may specify; or
 - 3.2.3 such other checks for the Supplier Staff of Sub-contractors as the Buyer may specify.

Exception for certain Sub-contractors

- 3.3 Where the Supplier considers it cannot ensure that a Sub-contractor will undertake the relevant security checks on any Sub-contractor Personnel, it must:
 - 3.3.1 as soon as practicable, and in any event within [20] Working Days of becoming aware of the issue, notify the Buyer;

- 3.3.2 provide such information relating to the Sub-contractor, its vetting processes and the roles the affected Supplier Staff will perform as the Buyer reasonably requires; and
- 3.3.3 comply, at the Supplier's cost, with all directions the Buyer may provide concerning the vetting of the affected Supplier Staff and the management of the Sub-contractor.

Annual training

- 3.4 The Supplier must ensure, and ensure that Sub-contractors ensure, that all Supplier Staff, complete and pass security training at least once every calendar year that covers:
 - 3.4.1 general training concerning security and data handling;
 - 3.4.2 Phishing, including the dangers from ransomware and other malware; and
 - 3.4.3 the Secure by Design Principles.

Staff access

- 3.5 The Supplier must ensure, and ensure that Sub-contractors ensure, that individual Supplier Staff can access only the Government Data necessary to allow individuals to perform their role and fulfil their responsibilities in the provision of the Services.
- 3.6 The Supplier must ensure, and ensure that Sub-contractors ensure, that where individual Supplier Staff no longer require access to the Government Data or any part of the Government Data, their access to the Government Data or that part of the Government Data is revoked immediately when their requirement to access Government Data ceases.
- 3.7 Where requested by the Buyer, the Supplier must remove, and must ensure that Sub-contractors remove, an individual Supplier Staff's access to the Government Data, or part of that Government Data specified by the Buyer, as soon as practicable and in any event within 24 hours of the request.

Remote Working

- 3.8 The Supplier must ensure, and ensure that Sub-contractors ensure, that:
 - 3.8.1 Unless agreed otherwise in writing by the Buyer, Privileged Users do not undertake Remote Working;
 - 3.8.2 where the Buyer 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 Buyer.
- 3.9 Where the Supplier or a Sub-contractor wishes to permit Supplier Staff to undertake Remote Working, it must:
 - 3.9.1 prepare and have approved by the Buyer the Remote Working Policy in accordance with this Paragraph;

- 3.9.2 undertake and, where applicable, ensure that any relevant Sub-contractors undertake, all steps required by the Remote Working Policy;
- 3.9.3 ensure that Supplier Staff undertake Remote Working only in accordance with the Remote Working Policy;
- 3.9.4 may not permit any Supplier Staff of the Supplier or any Sub-contractor to undertake Remote Working until the Remote Working Policy is approved by the Buyer.
- 3.10 The Remote Working Policy must include or make provision for the following matters:
 - 3.10.1 restricting or prohibiting Supplier Staff from printing documents in any Remote Location;
 - 3.10.2 restricting or prohibiting Supplier Staff from downloading any Government Data to any End-user Device other than an End-user Device that:
 - (a) is provided by the Supplier or Sub-contractor (as appropriate); and
 - (b) complies with the requirements set out in Paragraph 4 (*End-user Devices*);
 - 3.10.3 ensuring that Supplier Staff comply with the Expected Behaviours (so far as they are applicable);
 - 3.10.4 giving effect to the Security Controls (so far as they are applicable);
 - 3.10.5 for each different category of Supplier Staff subject to the proposed Remote Working Policy:
 - (a) 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;
 - (b) any identified security risks arising from the proposed Handling in a Remote Location;
 - (c) the mitigations, controls and security measures the Supplier or Sub-contractor (as applicable) will implement to mitigate the identified risks;
 - (d) the residual risk levels following the implementation of those mitigations, controls and measures;
 - (e) when the Supplier or Sub-contractor (as applicable) will implement the proposed mitigations, controls and measures; and
 - (f) the business rules with which the Supplier Staff must comply; and
 - 3.10.6 how the Supplier or the Sub-contractor (as applicable) will:

- (a) communicate the Remote Working Policy and business rules to Supplier Staff; and
 - (b) enforce the Remote Working Plan and business rules.
- 3.11 The Supplier may submit a proposed Remote Working Policy to the Buyer for consideration at any time.
- 3.12 The Buyer must, within 20 Working Days of the submission of a proposed Remote Working Plan, either:
 - 3.12.1 approve the proposed Remote Working Policy, in which case the Supplier must, and ensure that any applicable Sub-contractor, implements the approved Remote Working Plan in accordance with its terms;
 - 3.12.2 reject the proposed Remote Working Policy, in which case:
 - (a) the Buyer may set out any changes to the proposed Remote Working Policy the Buyer requires to make the plan capable of approval; and
 - (b) the Supplier may:
 - (i) revise the proposed Remote Working Plan; and
 - (ii) re-submit the proposed Remote Working Plan to the Buyer for approval under Paragraph 3.11.

4 End-user Devices

- 4.1 The Supplier must manage, and must ensure that all Sub-contractors manage, all End-user Devices on which Government Data or Code is stored or Handled in accordance the following requirements:
 - 4.1.1 the operating system and any applications that store, Handle or have access to Government Data or Code must be in current support by the vendor, or the relevant community in the case of open source operating systems or applications;
 - 4.1.2 users must authenticate before gaining access;
 - 4.1.3 all Government Data and Code must be encrypted using an encryption tool agreed to by the Buyer;
 - 4.1.4 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;
 - 4.1.5 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 and Code to ensure the security of that Government Data and Code;
 - 4.1.6 the Supplier or Sub-contractor, as applicable, can, without physical access to the End-user Device, remove or make inaccessible all

Government Data or Code stored on the device and prevent any user or group of users from accessing the device;

4.1.7 all End-user Devices are within the scope of any Relevant Certification.

4.2 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 the Contract.

4.3 Where there is any conflict between the requirements of this Schedule and the requirements of the NCSC Device Guidance, the requirements of this Schedule take precedence.

5 Hardware and software support

5.1 Before using any software as part of the Supplier Information Management System, the Supplier must:

5.1.1 perform adequate due diligence to determine whether there are any recognised security vulnerabilities with that software; and

5.1.2 where there are any recognised security vulnerabilities, either:

(a) remedy vulnerabilities; or

(b) ensure that the design of the Supplier Information Management System mitigates those vulnerabilities.

5.2 The Supplier must ensure that all software used to provide the Services remains at all times in full security support, including any extended or bespoke security support.

5.3 The Supplier must produce and maintain a register of all software that forms the Supplier Information Management System (**Support Register**).

5.4 The Support Register must include in respect of each item of software:

5.4.1 any vulnerabilities identified with the software and the steps the Supplier has taken to remedy or mitigate those vulnerabilities;

5.4.2 the date, so far as it is known, that the item will cease to be in mainstream security support; and

5.4.3 the Supplier's plans to upgrade the item before it ceases to be in mainstream security support.

5.5 The Supplier must:

5.5.1 review and update the Support Register:

(a) within ten Working days of becoming aware of any new vulnerability in any item of software;

(b) within ten Working Days of becoming aware of the date on which, or any change to the date on which, any item of software will cease to be in mainstream security report;

- (c) within ten Working Days of introducing new software, or removing existing software, from the Supplier Information Management System; and
 - (d) at least once every 12 months;
- 5.5.2 provide the Buyer with a copy of the Support Register:
 - (a) whenever it updates the Support Register; and
 - (b) otherwise when the Buyer requests.
- 5.6 Where any element of the Supplier Information Management System consists of COTS Software, the Supplier shall ensure:
 - 5.6.1 those elements are always in mainstream or extended security support from the relevant vendor; and
 - 5.6.2 the COTS Software is not more than one version or major release behind the latest version of the software.
- 5.7 The Supplier shall ensure that all hardware used to provide the Services, whether used by the Supplier or any Sub-contractor is, at all times, remains in mainstream vendor support, that is, that in respect of the hardware, the vendor continues to provide:
 - 5.7.1 regular firmware updates to the hardware; and
 - 5.7.2 a physical repair or replacement service for the hardware.
- 5.8 The Supplier must ensure that where any software or hardware component of the Supplier Information Management System is no longer required to provide the Services or has reached the end of its life it is removed or disconnected from the Supplier Information Management System.

6 Encryption

- 6.1 Before Handling any Government Data, the Supplier must agree with the Buyer the encryption methods that it and any Sub-contractors that Handle Government Data will use to comply with this Paragraph 6.
- 6.2 Where this Paragraph 6 requires Government Data to be encrypted, the Supplier must use, and ensure that Sub-contractors use, the methods agreed by the Buyer under Paragraph 6.1.
- 6.3 Unless Paragraph 6.4 applies, the Supplier must ensure, and must ensure that all Sub-contractors ensure, that Government Data is encrypted:
 - 6.3.1 when stored at any time when no operation is being performed on it, including when stored on any portable storage media; and
 - 6.3.2 when transmitted.
- 6.4 Where the Supplier, or a Sub-contractor, cannot encrypt Government Data as required by Paragraph 6.2, the Supplier must:
 - 6.4.1 immediately inform the Buyer of the subset or subsets of Government Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;

- 6.4.2 provide details of the protective measures the Supplier or Sub-contractor (as applicable) proposes to take to provide equivalent protection to the Buyer as encryption;
- 6.4.3 provide the Buyer with such additional information relating to the information provided under Paragraphs 6.4.1 and 6.4.2 as the Buyer may require.
- 6.5 The Buyer, the Supplier and, where the Buyer requires, any relevant Sub-contractor shall meet to agree appropriate protective measures for the unencrypted Government Data.
- 6.6 Where the Buyer and Supplier reach agreement, the Supplier must update the Security Management Plan to include:
 - 6.6.1 the subset or subsets of Government Data not encrypted and the circumstances in which that will occur;
 - 6.6.2 the protective measure that the Supplier and/or Sub-contractor will put in place in respect of the unencrypted Government Data.
- 6.7 Where the Buyer and Supplier do not reach agreement within 40 Working Days of the date on which the Supplier first notified the Buyer that it could not encrypt certain Government Data, either party may refer the matter to be determined by an expert in accordance with the Dispute Resolution Procedure.

7 Backup and recovery of Government Data

Backups and recovery of Government Data

- 7.1 The Supplier must backup and recover the Government Data in accordance with the Backup and Recovery Plan to ensure the recovery point objective and recovery time objective in Paragraph 7.3.1.
- 7.2 Any backup system operated by the Supplier or Sub-contractor forms part of the Supplier System or that Sub-contractor's System to which this Schedule and the security requirements in Appendix 1 apply.

Backup and Recovery Plan

- 7.3 Unless otherwise required by the Buyer, the Backup and Recovery Plan must provide for:
 - 7.3.1 in the case of a full or partial failure of the Supplier System or a Sub-contractor's System:
 - (a) a recovery time objective of **[Buyer guidance: insert period]**; and
 - (b) a recovery point objective of **[Buyer guidance: insert period]**; and
 - 7.3.2 a retention period of **[Buyer guidance: insert period]**.
- 7.4 In doing so, the Backup and Recovery Plan must ensure that in respect of any backup system operated by the Supplier or a Sub-contractor:

- 7.4.1 the backup location for Government Data is sufficiently physically and logically separate from the rest of the Supplier System or a Sub-contractor's System that it is not affected by any Disaster affecting the rest of the Supplier System or a Sub-contractor's System;
- 7.4.2 there is sufficient storage volume for the amount of Government Data to be backed up;
- 7.4.3 all back-up media for Government Data is used in accordance with the manufacturer's usage recommendations;
- 7.4.4 newer backups of Government Data do not overwrite existing backups made during the retention period specified in Paragraph 7.3.1(b);
- 7.4.5 the backup system monitors backups of Government Data to:
 - (a) identifies any backup failure; and
 - (b) confirm the integrity of the Government Data backed up;
- 7.4.6 any backup failure is remedied promptly;
- 7.4.7 the backup system monitors the recovery of Government Data to:
 - (a) identify any recovery failure;
 - (b) confirm the integrity of Government Data recovered; and
- 7.4.8 any recovery failure is promptly remedied.

8 Email

- 8.1 The Supplier must ensure that where the Supplier Information Management System will provide an Email Service to the Buyer, it:
 - 8.1.1 supports transport layer security (**TLS**) version 1.2, or higher, for sending and receiving emails;
 - 8.1.2 supports TLS Reporting (**TLS-RPT**);
 - 8.1.3 is capable of implementing:
 - (a) domain -based message authentication, reporting and conformance (**DMARC**);
 - (b) sender policy framework (**SPF**); and
 - (c) domain keys identified mail (**DKIM**); and

- 8.1.4 is capable of complying in all respects with any guidance concerning email security as issued or updated from time to time by:
- (a) the UK Government (current version at <https://www.gov.uk/guidance/set-up-government-email-services-securely>; or
 - (b) the NCSC (current version at <https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing>).

9 DNS

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

10 Malicious Software

- 10.1 The Supplier shall install and maintain Anti-virus Software or procure that Anti-virus Software is installed and maintained on the Supplier Information Management System.
- 10.2 The Supplier must ensure that such Anti-virus Software:
- 10.2.1 prevents the installation of the most common forms of Malicious Software in the Supplier Information Management System and the Development Environment;
 - 10.2.2 is configured to perform automatic software and definition updates;
 - 10.2.3 provides for all updates to be the Anti-virus Software to be deployed within [ten] Working Days of the update's release by the vendor;
 - 10.2.4 performs regular scans of the Supplier Information Management System to check for and prevent the introduction of Malicious Software; and
 - 10.2.5 where Malicious Software has been introduced into the Supplier Information Management System, identifies, contains the spread of, and minimises the impact of Malicious Software.
- 10.3 If Malicious Software is found, the Parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Government Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.

- 10.4 Any Breach of Security caused by Malicious Software where the Breach of Security arose from a failure by the Supplier, or a Sub-contractor, to comply with this Paragraph 10 is a material Default.

11 Vulnerabilities

- 11.1 Unless the Buyer otherwise agrees, the Supplier must ensure that it or any relevant Sub-contractor applies security patches to any vulnerabilities in the Supplier Information Management System no later than:
- 11.1.1 seven days after the public release of patches for vulnerabilities classified as "critical";
 - 11.1.2 30 days after the public release of patches for vulnerabilities classified as "important"; and
 - 11.1.3 60 days after the public release of patches for vulnerabilities classified as "other".
- 11.2 The Supplier must:
- 11.2.1 scan the Supplier Information Management System and the Development Environment at least once every month to identify any unpatched vulnerabilities; and
 - 11.2.2 if the scan identifies any unpatched vulnerabilities ensure they are patched in accordance with Paragraph 11.1.
- 11.3 For the purposes of this Paragraph 11, the Supplier must implement a method for classifying vulnerabilities to the Supplier Information Management System as "critical", "important" or "other" that is aligned to recognised vulnerability assessment systems, such as:
- 11.3.1 the National Vulnerability Database's vulnerability security ratings; or
 - 11.3.2 Microsoft's security bulletin severity rating system.

12 Security testing

Responsibility for security testing

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

Security tests by Supplier

- 12.2 The Supplier must:
- 12.2.1 before submitting the draft Security Management Plan to the Buyer for a decision under Paragraph 15;
 - 12.2.2 at least once during each Contract Year; and
 - 12.2.3 when required to do so by the Buyer;

undertake the following activities:

- 12.2.4 conduct security testing of the Supplier Information Management System (**IT Health Check**) in accordance with Paragraph 12.8 to 12.10; and
 - 12.2.5 implement any findings, and remedy any vulnerabilities identified by the IT Health Check in accordance with Paragraphs 12.11 to 12.21.
- 12.3 In addition to its obligations under Paragraph 12.2, the Supplier must undertake any tests required by:
- 12.3.1 any Remediation Action Plan;
 - 12.3.2 the ISO27001 Certification Requirements;
 - 12.3.3 the Security Management Plan; and
 - 12.3.4 the Buyer, following a Breach of Security or a significant change, as assessed by the Buyer, to the components or architecture of the Supplier Information Management System,
- (each a **Supplier Security Test**).
- 12.4 The Supplier must:
- 12.4.1 design and implement the Supplier Security Tests so as to minimise the impact on the delivery of the Services;
 - 12.4.2 agree the date, timing, content and conduct of such Supplier Security Tests in advance with the Buyer.
- 12.5 Where the Supplier fully complies with Paragraph 12.4, if a Supplier Security Test causes a Performance Failure in a particular Measurement Period, the Supplier shall be entitled to relief in respect of such Performance Failure for that Measurement Period.
- 12.6 The Buyer may send a representative to witness the conduct of the Supplier Security Tests.
- 12.7 The Supplier shall provide the Buyer with a full, unedited and unredacted copy of the results of such Security Tests (in a form approved by the Buyer in advance) as soon as practicable, and in any case within ten Working Days, after completion of each Supplier Security Test

IT Health Checks

- 12.8 In arranging an IT Health Check, the Supplier must:
- 12.8.1 use only a CHECK Service Provider to perform the IT Health Check;
 - 12.8.2 ensure that the CHECK Service Provider uses a qualified CHECK Team Leader and CHECK Team Members to perform the IT Health Check;
 - 12.8.3 design and plan for the IT Health Check so as to minimise the impact of the IT Health Check on the Supplier Information Management System and the delivery of the Services.

- 12.8.4 promptly provide the Buyer with such technical and other information relating to the Information Management System as the Buyer requests;
- 12.8.5 include within the scope of the IT Health Check such tests as the Buyer requires;
- 12.8.6 agree with the Buyer the scope, aim and timing of the IT Health Check.
- 12.9 The Supplier must commission the IT Health Check in accordance with the scope, aim and timing agreed by the Buyer.
- 12.10 Following completion of an IT Health Check, the Supplier must provide the Buyer with a full, unedited and unredacted copy of the report relating to the IT Health Check without delay and in any event within ten Working Days of its receipt by the Supplier.

Remedying vulnerabilities

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

Responding to a Security Test report

- 12.13 Where the Security Test report identifies vulnerabilities in, or makes findings in respect of, the Supplier Information Management System, the Supplier must within [20] Working Days of receiving the Security Test report, prepare and submit for approval to the Buyer a draft plan addressing the vulnerabilities and findings (**Remediation Action Plan**).
- 12.14 Where the Buyer has commissioned a root cause analysis under Paragraph 12.21, the Supplier shall ensure that the draft Remediation Action Plan addresses that analysis.
- 12.15 The draft Remediation Action Plan must, in respect of each vulnerability identified or finding made by the Security Test report:
 - 12.15.1 how the vulnerability or finding will be remedied;
 - 12.15.2 the date by which the vulnerability or finding will be remedied;
 - and

- 12.15.3 the tests that the Supplier proposes to perform to confirm that the vulnerability has been remedied or the finding addressed.
- 12.16 The Supplier shall promptly provide the Buyer with such technical and other information relating to the Supplier Information Management System, the IT Health Check report or the draft Remediation Action Plan as the Buyer requests.
- 12.17 The Buyer may:
- 12.17.1 reject the draft Remediation Action Plan where it considers that the draft Remediation Action Plan is inadequate, providing its reasons for doing so, in which case:
- (a) the Supplier shall within ten Working Days of the date on which the Buyer rejected the draft Remediation Action Plan submit a revised draft Remediation Action Plan that takes into account the Buyer's reasons; and
 - (b) Paragraph 12.15 to 12.17 shall apply, with appropriate modifications, to the revised draft Remediation Action Plan;
- 12.17.2 accept the draft Remediation Action Plan, in which case the Supplier must immediately start work on implementing the Remediation Action Plan in accordance with Paragraph 12.19 and 12.20.
- 12.18 Where the Buyer unreasonably:
- 12.18.1 delays its approval; or
- 12.18.2 rejects,
- the draft Remediation Action Plan, the Supplier will not be in breach of the Contract to the extent it demonstrates that any breach:
- 12.18.3 arose directly from the Buyer unreasonably withholding or delaying, as appropriate, its approval of the draft Remediation Action Plan; and
- 12.18.4 would not have occurred had:
- (a) the Buyer given its approval, or given its approval in a timely manner, to the draft Remediation Action Plan; and
 - (b) the Supplier had implemented the draft Remediation Action Plan in accordance with its terms.

Implementing an approved Remediation Action Plan

- 12.19 In implementing the Remediation Action Plan, the Supplier must conduct such further tests on the Supplier Information Management System as are required by the Remediation Action Plan to confirm that the Remediation Action Plan has fully and correctly implemented.
- 12.20 If any such testing identifies a new risk, new threat, vulnerability or exploitation technique with the potential to affect the security of the Supplier

Information Management System, the Supplier shall within two Working Days of becoming aware of such risk, threat, vulnerability or exploitation technique:

- 12.20.1 provide the Buyer with a full, unedited and unredacted copy of the test report;
- 12.20.2 implement interim mitigation measures to vulnerabilities in the Information System known to be exploitable where a security patch is not immediately available;
- 12.20.3 as far as practicable, remove or disable any extraneous interfaces, services or capabilities not needed for the provision of the Services within the timescales set out in the test report or such other timescales as may be agreed with the Buyer.

Significant vulnerabilities

12.21 Where:

- 12.21.1 a Security Test report identifies more than 10 vulnerabilities classified as either critical or high; or
- 12.21.2 the Buyer rejected a revised draft Remediation Action Plan, the Buyer may, at the Supplier's cost, either:
 - 12.21.3 appoint an independent and appropriately qualified and experienced security architect and adviser to perform a root cause analysis of the identified vulnerabilities; or
 - 12.21.4 give notice to the Supplier requiring the appointment as soon as reasonably practicable, and in any event within ten Working Days, of an Independent Security Adviser.

13 Access Control

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

- 13.1.1 identify and authenticate all persons who access the Supplier Information Management System and Sites before they do so;
- 13.1.2 require multi-factor authentication for all user accounts that have access to Government Data or that are Privileged Users;
- 13.1.3 allow access only to those parts of the Supplier Information Management System and Sites that those persons require;
- 13.1.4 maintain records detailing each person's access to the Supplier Information Management System and Sites, and make those records available to the Buyer on request.

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

- 13.2.1 are allocated to a single, individual user;

- 13.2.2 are accessible only from dedicated End-user Devices;
- 13.2.3 are configured so that those accounts can only be used for system administration tasks;
- 13.2.4 require passwords with high complexity that are changed regularly;
- 13.2.5 automatically log the user out of the Supplier Information Management System after a period of time that is proportionate to the risk environment during which the account is inactive; and
- 13.2.6 are:
 - (a) restricted to a single role or small number of roles;
 - (b) time limited; and
 - (c) restrict the Privileged User's access to the internet.
- 13.3 The Supplier must ensure, and must ensure that all Sub-contractors ensure, that it logs all activity of the Privileged Users while those users access those accounts and keeps the activity logs for 20 Working Days before deletion.
- 13.4 The Supplier must require, and must ensure that all Sub-contractors require, that Privileged Users use unique and substantially different high-complexity passwords for their different accounts on the Supplier Information Management System.
- 13.5 The Supplier must, and must ensure that all Sub-contractors:
 - 13.5.1 configure any hardware that forms part of the Supplier Information Management System that is capable of requiring a password before it is accessed to require a password; and
 - 13.5.2 change the default password of that hardware to a password of high complexity that is substantially different from the password required to access similar hardware.

14 Event logging and protective monitoring

Protective Monitoring System

- 14.1 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 Information Management System, the Development Environment, the Government Data and the Code to:
 - 14.1.1 identify and prevent potential Breaches of Security;
 - 14.1.2 respond effectively and in a timely manner to Breaches of Security that do occur;
 - 14.1.3 identify and implement changes to the Supplier Information Management System to prevent future Breaches of Security; and
 - 14.1.4 help detect and prevent any potential criminal offence relating to fraud, bribery or corruption using the Supplier Information Management System,

(Protective Monitoring System).

- 14.2 The Protective Monitoring System must provide for:
- 14.2.1 event logs and audit records of access to the Supplier Information Management system; and
 - 14.2.2 regular reports and alerts to identify:
 - (a) changing access trends;
 - (b) unusual usage patterns; or
 - (c) the access of greater than usual volumes of Government Data;
 - 14.2.3 the detection and prevention of any attack on the Supplier Information Management System or the Development Environment using common cyber-attack techniques;
 - 14.2.4 any other matters required by the Security Management Plan.

Event logs

- 14.3 The Supplier must ensure that, unless the Buyer otherwise agrees, any event logs do not log:
- 14.3.1 personal data, other than identifiers relating to users; or
 - 14.3.2 sensitive data, such as credentials or security keys.

Provision of information to Buyer

- 14.4 The Supplier must provide the Buyer on request with:
- 14.4.1 full details of the Protective Monitoring System it has implemented; and
 - 14.4.2 copies of monitoring logs and reports prepared as part of the Protective Monitoring System.

Changes to Protective Monitoring System

- 14.5 The Buyer may at any time require the Supplier to update the Protective Monitoring System to:
- 14.5.1 respond to a specific threat identified by the Buyer;
 - 14.5.2 implement additional audit and monitoring requirements; and
 - 14.5.3 stream any specified event logs to the Buyer's security information and event management system.

15 Audit rights

Right of audit

- 15.1 The Buyer may undertake an audit of the Supplier or any Sub-contractor to:
- 15.1.1 verify the Supplier's or Sub-contractor's (as applicable) compliance with the requirements of this Schedule and the Data Protection Laws as they apply to Government Data;
 - 15.1.2 inspect the Supplier Information Management System (or any part of it);

- 15.1.3 review the integrity, confidentiality and security of the Government Data; and/or
- 15.1.4 review the integrity and security of the Code.
- 15.2 Any audit undertaken under Paragraph 15.1:
 - 15.2.1 may only take place during the Contract Period and for a period of 18 months afterwards; and
 - 15.2.2 is in addition to any other rights of audit the Buyer has under the Contract.
- 15.3 The Buyer may not undertake more than one audit under Paragraph 15.1 in each calendar year unless the Buyer has reasonable grounds for believing:
 - 15.3.1 the Supplier or any Sub-contractor has not complied with its obligations under the Contract or the Data Protection Laws as they apply to the Government Data;
 - 15.3.2 there has been or is likely to be a Breach of Security affecting the Government Data or the Code; or
 - 15.3.3 where vulnerabilities, or potential vulnerabilities, in the Code have been identified by:
 - (a) an IT Health Check; or
 - (b) a Breach of Security.

Conduct of audits

- 15.4 The Buyer must use reasonable endeavours to provide 15 Working Days' notice of an audit.
- 15.5 The Buyer must when conducting an audit:
 - 15.5.1 comply with all relevant policies and guidelines of the Supplier or Sub-contractor (as applicable) concerning access to the Supplier Information Management System the Buyer considers reasonable having regard to the purpose of the audit; and
 - 15.5.2 use reasonable endeavours to ensure that the conduct of the audit does not unreasonably disrupt the Supplier or Sub-contractor (as applicable) or delay the provision of the Services.
- 15.6 The Supplier must, and must ensure that Sub-contractors, on demand provide the Buyer with all co-operation and assistance the Buyer may reasonably require, including:
 - 15.6.1 all information requested by the Buyer within the scope of the audit;
 - 15.6.2 access to the Supplier Information Management System; and
 - 15.6.3 access to the Supplier Staff.

Response to audit findings

15.7 Where an audit finds that:

15.7.1 the Supplier or a Sub-contractor has not complied with the Contract or the Data Protection Laws as they apply to the Government Data; or

15.7.2 there has been or is likely to be a Security Breach affecting the Government Data

the Buyer may require the Supplier to remedy those defaults at its own cost and expense and within the time reasonably specified by the Buyer.

15.8 The exercise by the Buyer of any rights it may have under this Paragraph 15 does not affect the exercise by it of any other or equivalent rights it may have under the Contract in respect of the audit findings.

16 Breach of Security

Reporting Breach of Security

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

Immediate steps

16.2 The Supplier must, upon becoming aware of a Breach of Security immediately take those steps identified in the Security Management Plan and all other steps reasonably necessary to:

16.2.1 minimise the extent of actual or potential harm caused by such Breach of Security;

16.2.2 remedy such Breach of Security to the extent possible;

16.2.3 apply a tested mitigation against any such Breach of Security; and

16.2.4 prevent a further Breach of Security in the future which exploits the same root cause failure;

Subsequent action

16.3 As soon as reasonably practicable and, in any event, within five Working Days of the occurrence of the Breach of Security, or such other period specified by the Buyer, provide to the Buyer:

16.3.1 full details of the Breach of Security; and

16.3.2 if required by the Buyer:

(a) a root cause analysis; and

(b) a draft plan addressing the Breach of Security,

(a **Breach Action Plan**).

16.4 The draft Breach Action Plan must set out:

16.4.1 in respect of each issue identified in the root cause analysis:

(a) how the issue will be remedied;

- (b) the date by which the issue will be remedied; and
 - (c) the tests that the Supplier proposes to perform to confirm that the issue has been remedied or the finding addressed;
- 16.4.2 the assistance the Supplier will provide to the Buyer to resolve any impacts on the Buyer, the Government Data and the Code;
- 16.4.3 the Supplier's communication and engagement activities in respect of the Breach of Security, including any communication or engagement with individuals affected by any Breach of Security that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data; and
- 16.4.4 the infrastructure, services and systems (including any contact centre facilities) the Supplier will establish to undertake the remediation, communication and engagement activities.
- 16.5 The Supplier shall promptly provide the Buyer with such technical and other information relating to the draft Breach Action Plan as the Buyer requests.
- 16.6 The Buyer may:
 - 16.6.1 reject the draft Breach Action Plan where it considers that the draft Breach Action Plan is inadequate, providing its reasons for doing so, in which case:
 - (a) the Supplier shall within ten Working Days of the date on which the Buyer rejected the draft Breach Action Plan, or such other period as the Buyer requires, submit a revised draft Breach Action Plan that takes into account the Buyer's reasons; and
 - (b) Paragraph 16.5 and 16.6 shall apply to the revised draft Breach Action Plan; or
 - 16.6.2 accept the draft Breach Action Plan, in which case the Supplier must immediately start work on implementing the Breach Action Plan.
- 16.7 When implementing the Breach Action Plan, the Supplier must:
 - 16.7.1 establish infrastructure, services and systems referred to in the Breach Action Plan;
 - 16.7.2 communicate and engage with affected individuals in accordance with the Breach Action Plan;
 - 16.7.3 communicate and engage with the Buyer and stakeholders identified by the Buyer in accordance with the Breach Plan and as otherwise required by the Buyer; and
 - 16.7.4 engage and deploy such additional resources as may be required to perform its responsibilities under the Breach Plan and the Contract in respect of the Personal Data Breach without any impact on the provision of the Services;
 - 16.7.5 continue to implement the Breach Action Plan until the Buyer indicates that the Breach of Security and the impacts on the Buyer, the

Government Data, the Code and the affected individuals have been resolved to the Buyer's satisfaction.

- 16.8 The obligation to provide and implement a Breach Action Plan under Paragraphs 16.3 to 16.7 continues notwithstanding the expiry or termination of the Contract.

Costs of preparing and implementing Breach Action Plan

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

Reporting of Breach of Security to regulator

- 16.10 Where the Law requires the Supplier report a Breach of Security to the appropriate regulator, the Supplier must:

16.10.1 make that report within the time limits:

- (a) specified by the relevant regulator; or
- (b) otherwise required by Law; and

16.10.2 to the extent that the relevant regulator or the Law permits, provide the Buyer with a full, unredacted and unedited copy of that report at the same time it is sent to the relevant regulator.

- 16.11 Where the Law requires the Buyer to report a Breach of Security to the appropriate regulator, the Supplier must:

16.11.1 provide such information and other input as the Buyer requires within the timescales specified by the Buyer; and

16.11.2 ensure so far as practicable the report it sends to the relevant regulator is consistent with the report provided by the Buyer.

17 Exit management

- 17.1 In addition to any obligations on the Supplier under Call-Off Schedule 10 (*Exit Management*) the Supplier must:

17.1.1 agree with the Buyer and, where required by the Supplier, the Replacement Supplier; and

17.1.2 document as part of the Exit Plan,

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

- 17.2 The Data Migration Plan must, at a minimum, include:

17.2.1 the data formats of the Government Data;

17.2.2 the roles and responsibilities of the Supplier, the Buyer and (where applicable) the Replacement Supplier;

17.2.3 the methods to be used to securely transfer the data;

17.2.4 the timescales for the completion of all tasks and activities set out in the Data Migration Plan; and

- 17.2.5 how data migration will be managed to ensure continuity of Services and the integrity, confidentiality and accessibility of the Government Data during that process.
- 17.3 The Supplier shall comply with the provisions of the Data Migration Plan during Exit Management.
- 18 Return and deletion of Government Data**
- 18.1 The Supplier must create and maintain a register of:
- 18.1.1 all Government Data the Supplier, or any Sub-contractor, receives from or creates for the Buyer; and
- 18.1.2 those parts of the Supplier Information Management System, including those parts of the Supplier Information Management System that are operated or controlled by any Sub-contractor, on which the Government Data is stored,
- (Government Data Register).**
- 18.2 The Supplier must:
- 18.2.1 review and update the Government Data Register:
- (a) within ten Working Days of the Supplier or any Sub-contractor changes those parts of the Supplier Information Management System on which the Government Data is stored;
 - (b) within ten Working Days of a significant change in the volume, nature or overall sensitivity of the Government Data stored on the Supplier Information Management System;
 - (c) at least once every 12 months; and
- 18.2.2 provide the Buyer with a copy of the Government Data Register:
- (a) whenever it updates the Government Data Register; and
 - (b) otherwise when the Buyer requests.
- 18.3 Subject to Paragraph 18.4, the Supplier must, and must ensure that all Sub-contractors, securely erase any or all Government Data held by the Supplier or Sub-contractor, including any or all Code:
- 18.3.1 when requested to do so by the Buyer; and
- 18.3.2 using a deletion method agreed with the Buyer that ensures that even a determined expert using specialist techniques can recover only a small fraction of the data deleted.
- 18.4 Paragraph 18.3 does not apply to Government Data:
- 18.4.1 that is Personal Data in respect of which the Supplier is a Controller;
- 18.4.2 to which the Supplier has rights to Handle independently from the Contract; or
- 18.4.3 in respect of which, the Supplier is under an obligation imposed by Law to retain.

- 18.5 The Supplier must, and must ensure that all Sub-contractors, provide the Buyer with copies of any or all Government Data held by the Supplier or Sub-contractor, including any or all Code:
- 18.5.1 when requested to do so by the Buyer; and
 - 18.5.2 using the method specified by the Buyer.

Appendix 2 Security requirements for Development Activity

1 Secure Software Development by Design

- 1.1 The Supplier must, and must ensure that all Sub-contractors engaged in Development Activity, implement secure development and deployment practices to ensure that:
 - 1.1.1 no Malicious Software is introduced into the Developed System or the Supplier Information Management System; and
 - 1.1.2 the Developed System can continue to function in accordance with the Specification:
 - (a) in unforeseen circumstances; and
 - (b) notwithstanding any attack on the Developed System using common cyber-attack techniques, including attacks using those vulnerabilities identified at any time in the OWASP Top Ten.
- 1.2 To those ends, the Supplier must, and ensure that all Sub-contractors engaged in Development Activity:
 - 1.2.1 comply with the Secure Development Guidance as if its requirements were terms of the Contract; and
 - 1.2.2 document the steps taken to comply with that guidance as part of the Security Management Plan.
- 1.3 In particular, the Supplier must, and ensure that all Sub-contractors engaged in Development Activity:
 - 1.3.1 ensure that all Supplier Staff engaged in Development Activity are:
 - (a) trained and experienced in secure by design code development; and
 - (b) provided with regular training in secure software development and deployment;
 - 1.3.2 ensure that all Code:
 - (a) is subject to a clear, well -organised, logical and documented architecture;
 - (b) follows OWASP Secure Coding Practice
 - (c) follows recognised secure coding standard, where one is available;
 - (d) employs consistent naming conventions;
 - (e) is coded in a consistent manner and style;
 - (f) is clearly and adequately documented to set out the function of each section of code; and

- (g) is subject to appropriate levels of review through automated and non-automated methods both as part of:
 - (i) any original coding; and
 - (ii) at any time the Code is changed; and

1.3.3 ensure that all Development Environments:

- (a) protect access credentials and secret keys;
- (b) is logically separate from all other environments, including production systems, operated by the Supplier or Sub-contractor;
- (c) requires multi-factor authentication to access;
- (d) have onward technical controls to protect the Developed System or the Supplier Information Management System in the event a Development Environment is compromised; and
- (e) use network architecture controls to constrain access from the Development Environment to the Developed System or the Supplier Information Management System.

2 Secure Architecture

- 2.1 The Supplier shall design and build the Developed System in a manner consistent with:
 - 2.1.1 the NCSC's guidance on "Security Design Principles for Digital Services";
 - 2.1.2 where the Developed System will Handle bulk data, the NCSC's guidance on "Bulk Data Principles"; and
 - 2.1.3 the NCSC's guidance on "Cloud Security Principles".
- 2.2 Where any of the documents referred to in Paragraph 2.1 provides for various options, the Supplier must document the option it has chosen to implement and its reasons for doing so.
- 2.3 Notwithstanding anything in the specification for the Developed System or the Contract, the Supplier must ensure that the Developed System encrypts Government Data:
 - 2.3.1 when the Government Data is stored at any time when no operation is being performed on it; and
 - 2.3.2 when the Government Data is transmitted.
- 2.4 The Supplier must ensure that the Developed System is developed and configured so as to provide for the matters set out in Paragraphs 13.1 to 13.4 of Appendix 1.

3 Code Repository and Deployment Pipeline

The Supplier must, and must ensure that all Sub-contractors engaged in Development Activity:

- 3.1 when using a cloud -based code repository for the deployment pipeline, use only a cloud -based code repository that has been assessed against the NCSC Cloud Security Principles;
- 3.2 ensure user access to code repositories is authenticated using credentials, with passwords or private keys;
- 3.3 ensure secret credentials are separated from source code.
- 3.4 run automatic security testing as part of any deployment of the Developed System.

4 Development and Testing Data

The Supplier must, and must ensure that all Sub-contractors engaged in Development Activity, use only anonymised, dummy or synthetic data when using data within the Development Environment for the purposes of development and testing.

5 Code Reviews

- 5.1 The Supplier must:

- 5.1.1 regularly; or

- 5.1.2 as required by the Buyer

review the Code in accordance with the requirements of this Paragraph 5 (**Code Review**).

- 5.2 Before conducting any Code Review, the Supplier must agree with the Buyer:

- 5.2.1 the modules or elements of the Code subject to the Code Review;

- 5.2.2 the development state at which the Code Review will take place;

- 5.2.3 any specific security vulnerabilities the Code Review will assess; and

- 5.2.4 the frequency of any Code Reviews,

(the **Code Review Plan**).

- 5.3 For the avoidance of doubt the Code Review Plan may specify different modules or elements of the Code are reviewed at a different development state, for different security vulnerabilities and at different frequencies.

- 5.4 The Supplier:

- 5.4.1 must undertake Code Reviews in accordance with the Code Review Plan; and

- 5.4.2 may undertake Code Reviews by automated means if this is consistent with the approach specified in the Code review Plan.

- 5.5 No later than ten Working Days after each Code Review, the Supplier must provide the Buyer will a full, unedited and unredacted copy of the Code Review Report.

- 5.6 Where the Code Review identifies any security vulnerabilities, the Supplier must:
- 5.6.1 remedy these at its own cost and expense;
 - 5.6.2 ensure, so far as reasonably practicable, that the identified security vulnerabilities are not present in any other modules or code elements; and
 - 5.6.3 modify its approach to undertaking the Development Activities to ensure, so far as is practicable, the identified security vulnerabilities will not re-occur; and
 - 5.6.4 provide the Buyer with such information as it requests about the steps the Supplier takes under this Paragraph 5.6.

6 Third-party Software

The Supplier must not, and must ensure that Sub-contractors do not, use any software to Handle Government Data where the licence terms of that software purport to grant the licensor rights to Handle the Government Data greater than those rights strictly necessary for the use of the software.

7 Third-party Software Modules

- 7.1 Where the Supplier or a Sub-contractor incorporates a Third-party Software Module into the Code, the Supplier must:
- 7.1.1 verify the source and integrity of the Third-party Software Module by cryptographic signing or such other measure that provides the same level of assurance;
 - 7.1.2 perform adequate due diligence to determine whether there are any recognised security vulnerabilities with that Third-party Software Module;
 - 7.1.3 continue to monitor any such Third-party Software Module so as to ensure it promptly becomes aware of any newly-discovered security vulnerabilities;
 - 7.1.4 take appropriate steps to minimise the effect of any such security vulnerability on the Developed System.
- 7.2 For the purposes of Paragraph 7.1.2, the Supplier must perform due diligence that is proportionate to the significance of the Third-party Software Module within the Code.
- 7.3 The Supplier must produce and maintain a register of all Third-party Software Modules that form part of the Code (**Modules Register**).
- 7.4 The Modules Register must include, in respect of each Third-party Software Module:
- 7.4.1 full details of the developer of the module;

- 7.4.2 the due diligence the Supplier undertook on the Third-party Software Module before deciding to use it;
 - 7.4.3 any recognised security vulnerabilities in the Third-party Software Module; and
 - 7.4.4 how the Supplier will minimise the effect of any such security vulnerability on the Developed System.
- 7.5 The Supplier must:
- 7.5.1 review and update the Modules Register:
 - (a) within [10] Working Days of becoming aware of a security vulnerability in any Third-party Software Module; and
 - (b) at least once every six months;
 - 7.5.2 provide the Buyer with a copy of the Modules Register:
 - (a) whenever it updates the Modules Register; and
 - (b) otherwise when the Buyer requests.

Appendix 3 Security Working Group

1 Role of the Security Working Group

- 1.1 The Security Working Group shall be responsible for the **[Buyer Guidance: insert remit of Security Working Group]**.
- 1.2 The Security Working Group:
 - 1.2.1 monitors and provides recommendations to the Supplier on the Buyer-led Assurance of the Supplier Information Management System;
 - 1.2.2 provides a forum for the sharing of information concerning security risks and threats and determining the appropriate mitigations;
 - 1.2.3 **[Buyer Guidance: insert any terms of reference for Security Working Group that the Buyer wishes to apply]**.

2 Meetings of the Security Working Group

Paragraph 4.4 of Call-Off Schedule 15 (*Contract Management*) shall apply to the Security Working Group and references to 'board' and 'Operational Board' shall be construed as references to the Security Working Group.

3 Reports to the Security Working Group

- 3.1 The Supplier must provide the following reports no later than **[five]** Working Days before each meeting of the Security Working Group:
 - 3.1.1 **[Buyer Guidance: insert list of required reports]**.

4 Administration

The Supplier is responsible for the secretarial functions of the SWG.

Appendix 4 Sub-contractor Security Requirements and Security Requirements for Development Activity

The table below sets out the security requirements in Appendix 1 and the security requirements for Development Activity in Appendix 2 that do **not** apply to particular categories of Sub-contractors.

[Buyer Guidance: Populate this table to reflect any provisions of Appendix 1 or Appendix 2 that will not apply to any particular categories of Sub-contractor]

	SIMS Sub-contractors	Higher-risk Sub-contractors	Medium-risk Sub-contractors	Sub-contractors
Appendix 1 security requirements that do not apply				
Appendix 2 security requirements for Development Activity that do not apply				

Appendix 5 Secure by Design Principles Evaluation Table

1 Completion of Principles Evaluation Table

- 1.1 As part of the Security Management Plan, the Supplier must complete the table in this Appendix 5 (*Secure by Design Principles Evaluation Table*), unless that requirement is waived by the Buyer.
- 1.2 In completing this table, the Supplier must set out how it and any Sub-contractors will meet the Secure by Design Principles.

Secure by Design Principle	Requirements	How the Supplier will meet the requirement
Principle 1 Create responsibility for cyber security risk Assign a designated risk owner to be accountable for managing cyber security risks for the service within the contract. This must be a senior stakeholder with the experience, knowledge and Buyer to lead on security activities.	The Supplier designates a senior individual within their organisation who has overall accountability for ensuring the Secure by Design are met as part of the overall security requirements stated within the contract.	
	The Supplier designates a senior individual within the supplier delivery team - who will be reporting to the SRO, service owner or equivalent - with overall responsibility for the management of cyber security risks of digital services and technical	

Secure by Design Principle	Requirements	How the Supplier will meet the requirement
	infrastructure during their delivery.	
	<p>The Supplier provides adequate and appropriately qualified resources to support the Buyer with following the government Secure by Design approach as part of service delivery.</p> <p>These resources must be reviewed at the beginning of each of the delivery phases during the delivery lifecycle of the service as agreed with the Buyer.</p>	
<p>Principle 2</p> <p>Source secure technology products</p> <p>Where third-party products are used, perform security due diligence by continually assessing platforms, software and code for</p>	<p>The Supplier carries out proportionate (risk-driven) security reviews of third-party products before they are considered as a component of the digital service. The type and details of the review should be based on the significance associated with</p>	

Secure by Design Principle	Requirements	How the Supplier will meet the requirement
security vulnerabilities. Mitigate risks and share findings with suppliers to help them improve product security.	the product and are subject to agreement with the Buyer.	
	The Supplier takes reasonable steps to reduce potential cyber security risks associated with using a third-party product as part of the service to a level that meets the Buyer's security risk appetite for the service. Where the risk cannot be mitigated to such level, the Buyer should be informed and asked to accept the risk associated with using the product.	
	The Supplier takes reasonable steps to assess third-party products used as a component of the digital service against legal and regulatory obligations and industry security standards specified by the Buyer. Where the product doesn't	

Secure by Design Principle	Requirements	How the Supplier will meet the requirement
	meet the required obligations, the Supplier must discuss with the Buyer the residual risks associated with using the product.	
Principle 3 Adopt a risk-driven approach Establish the project's risk appetite and maintain an assessment of cyber security risks to build protections appropriate to the evolving threat landscape.	As provided by the Buyer, the Supplier should share the risk appetite across the supplier's delivery team from the outset.	
	The Supplier supports the Buyer with identifying the cyber threats and attack paths as part of ongoing threat modelling during digital service delivery.	
	The Supplier supports the Buyer with assessing cyber security risks and providing risk analysis details to help risk owners make informed risk decisions. During the assessment, risks to the digital service are	

Secure by Design Principle	Requirements	How the Supplier will meet the requirement
	identified, analysed, prioritised, and appropriate mitigation is proposed taking into account the risk appetite during the lifecycle of the service.	
	The Supplier produces an output from the risk management process containing a clear set of security requirements that will reduce the risks in line with the agreed risk appetite and cyber security risk management approach.	
	The Supplier factors in the legal and regulatory requirements provided by the Buyer in the risk management process and service design and build.	
Principle 4	The Supplier ensures that security requirements that are	

Secure by Design Principle	Requirements	How the Supplier will meet the requirement
<p>Design usable security controls</p> <p>Perform regular user research and implement findings into service design to make sure security processes are fit for purpose and easy to understand.</p>	<p>defined and documented as part of user research activities (for example user stories and user journeys) are fed into the design of the digital service.</p>	
	<p>The Supplier ensures that business objectives informing security requirements listed in the business case for the digital service are taken into consideration when designing security controls.</p>	
<p>Principle 5</p> <p>Build in detect and respond security</p> <p>Design for the inevitability of security vulnerabilities and incidents. Integrate appropriate security logging, monitoring, alerting and response capabilities.</p>	<p>The Supplier responsible for building the digital service ensures that proportionate security logging, monitoring and alerting mechanisms able to discover cyber security events and vulnerabilities documented in the threat and risk assessment are designed into the service.</p>	

Secure by Design Principle	Requirements	How the Supplier will meet the requirement
These must be continually tested and iterated.	The Supplier responsible for building the digital service integrates incident response and recovery capabilities that are in line with the requirements and timescales documented in the service resilience or similar documentation.	
	The Supplier responsible for building the digital service regularly tests digital services and infrastructure to identify and fix weaknesses within systems.	
Principle 6 Design flexible architectures Implement digital services and update legacy components to allow for easier integration of new security controls in	As agreed with the Buyer, the Supplier responsible for building the digital service uses flexible architectures and components that allow integration of new security measures in response to changes in business	

Secure by Design Principle	Requirements	How the Supplier will meet the requirement
response to changes in business requirements, cyber threats and vulnerabilities.	requirements, cyber threats and vulnerabilities.	
	The Supplier responsible for building the digital service tests security controls and verifying they are fit for purpose before deployment.	
Principle 7 Minimise the attack surface Use only the capabilities, software, data and hardware components necessary for a service to mitigate cyber security risks while achieving its intended use.	The Supplier responsible for building the digital service implements risk-driven security controls which meet the risk appetite and appropriate baseline as agreed with the Buyer.	
	The Supplier responsible for building the digital service follows secure coding practices and, with consultation with the Buyer's delivery team, identifies and mitigates vulnerabilities proactively reducing the number of vulnerabilities that	

Secure by Design Principle	Requirements	How the Supplier will meet the requirement
	potential attackers can exploit.	
	The Supplier retires service components (including data) securely when they are no longer needed, or at the end of their lifecycle.	
Principle 8 Defend in depth Create layered controls across a service so it's harder for attackers to fully compromise the system if a single control fails or is overcome.	The Supplier responsible for building the digital service adopts a defence in depth approach when designing the security architecture for the digital service.	
	The Supplier responsible for building the digital service implements security measures to incorporate segmentation.	