# Schedule 5
# (*Security Management)*
# Supplier-led Assurance

# 1 Authority Options

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

| | | |
|---|---|---|
| **Authority Security Policies** (see Paragraph 5) | | |
| The Authority requires the Supplier to comply with the following policies relating to security management:<br>Not used | | ☐ |
| **Locations** (see Paragraph 1 of the Security Requirements) | | |
| The Supplier and Sub-contractors may store, access or Handle Government Data in: | the United Kingdom only | ☒ |
| | 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) | ☐ |
| | anywhere in the world not prohibited by the Authority | ☐ |
| **Support Locations** (see Paragraph 1 of the Security Requirements) | | |
| The Supplier and Subcontractors may operate Support Locations in: | the United Kingdom only | ☒ |
| | 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) | ☐ |
| | anywhere in the world not prohibited by the Authority | ☐ |
| **Development Activity** (see Appendix 2) | | |
| The Authority requires the Supplier to undertake Development Activity under this Contract and, as a consequence, Appendix 2 applies | | ☐ |
| **Locations for Development Activity** (applies only if the option relating to Development Activities is selected; see Paragraph 1 of the Security Requirements) | | |
| The Supplier and Subcontractors may undertake Development Activity in: | the United Kingdom only | ☐ |
| | 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) | |
| | anywhere in the world not prohibited by the Authority | ☐ |

## 2 Definitions

**The following defined terms used within this Schedule can be found within Schedule 1 (Definitions):**
Assets;
Authority Data;
Authority Premises;
Authority System;
EEA;
Key Subcontractor;
Malicious Software;
Sites;
Supplier Personnel; and
Supplier System.

| | |
|---|---|
| **Anti-virus Software** | means software that:<br>(a) protects the Supplier Information Management System from the possible introduction of Malicious Software;<br>(b) scans for and identifies possible Malicious Software in the Supplier Information Management System;<br>(c) if Malicious Software is detected in the Supplier Information Management System, so far as possible:<br>(i) prevents the harmful effects of the Malicious Software; and<br>(ii) removes the Malicious Software from the Supplier Information Management System. |
| **Authority Data Register** | means the register of all Authority Data the Supplier, or any Sub-contractor, receives from or creates for the Authority, produced and maintained in accordance with Paragraph 18 of the Security Requirements. |
| **Authority Equipment** | means any hardware, computer or telecoms devices, and equipment that forms part of the Authority System. |
| **Backup and Recovery Plan** | the section of the Security Management Plan setting out the Suppliers' and Sub-contractors' plans for the back and recovery of any Authority Data they Handle. |
| **Breach Action Plan** | means a plan prepared under Paragraph 16.3 of the Security Requirements addressing any Breach of Security. |

| | |
|---|---|
| **Breach of Security** | means the occurrence of:<br>(a) any unauthorised access to or use of the Services, the Authority Premises, the Sites, the Supplier Information Management System and/or any information or data used by the Authority, the Supplier or any Sub-contractor in connection with this Contract, including the Authority Data and the Code;<br>(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 Authority, the Supplier or any Sub-contractor in connection with this Contract, including the Authority Data and the Code; and/or<br>(c) any part of the Supplier Information Management System ceasing to be compliant with the Certification Requirements;<br>(d) the installation of Malicious Software in the:<br>(i) Supplier Information Management System;<br>(ii) Development Environment; or<br>(iii) Developed System;<br>(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:<br>(i) Supplier Information Management System;<br>(ii) Development Environment; or<br>(iii) Developed System; and<br>(f) includes any attempt to undertake the activities listed in sub-Paragraph (a) where the Supplier has reasonable grounds to suspect that attempt:<br>(i) was part of a wider effort to access information and communications technology operated by or on behalf of Central Government Bodies; or<br>(ii) was undertaken, or directed by, a state other than the United Kingdom. |
| **Certification Requirements** | means the requirements set out in Paragraph 13 |
| **CHECK Scheme** | means 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** | means a company which, under the CHECK Scheme:<br>(a) has been certified by the National Cyber Security Centre;<br>(b) holds "Green Light" status; and<br>(c) is authorised to provide the IT Health Check services required by Paragraph 12 of the Security Requirements. |

| | |
|---|---|
| **CHECK Team Leader** | means an individual with a CHECK Scheme team leader qualification issued by the NCSC. |
| **CHECK Team Member** | means an individual with a CHECK Scheme team member qualification issued by the NCSC. |
| **Code** | means, in respect of the Developed System:<br>(d) the source code;<br>(e) the object code;<br>(f) third-party components, including third-party coding frameworks and libraries; and<br>(g) all supporting documentation. |
| **Code Review** | means a periodic review of the Code by manual or automated means to:<br>(a) identify and fix any bugs; and<br>(a) ensure the Code complies with<br>(i) the requirements of this Schedule 5 (*Security Management*); and<br>(ii) the Secure Development Guidance. |
| **Code Review Plan** | means the document agreed with the Authority under Paragraph 5.2 of the Security Requirements for Development setting out the requirements for, and frequency of, Code Reviews. |
| **Code Review Report** | means a report setting out the findings of a Code Review. |
| **Cyber Essentials** | means the Cyber Essentials certificate issued under the Cyber Essentials Scheme. |
| **Cyber Essentials Plus** | means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme. |
| **Cyber Essentials Scheme** | means the Cyber Essentials scheme operated by the National Cyber Security Centre. |
| **Data Migration Plan** | means the plan for the migration of the Authority Data to the Authority and/or the Replacement Supplier (as required by the Authority) required by Paragraph 17 of the Security Requirements. |
| **Developed System** | means the software or system that the Supplier is required to develop under this Contract; |
| **Development Activity** | means any activity relating to the development, deployment maintenance and upgrading of the Developed System, including:<br>(a) coding;<br>(b) testing;<br>(c) code storage; and |

| | |
|---|---|
| | (d) deployment. |
| **Development Environment** | means 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. |
| **End-user Device** | means 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** | means a service that will send, or can be used to send, emails from the Authority's email address or otherwise on behalf of the Authority. |
| **Expected Behaviours** | means 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 Security Classification Policy** | means the policy, as updated from time to time, establishing an administrative system to protect information assets appropriately against prevalent threats, including classification tiers, protective security controls and baseline behaviours, the current version of which is found at https://www.gov.uk/government/publications/government-security-classifications |
| **Handle** | means any operation performed on data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of that data. |

| | |
|---|---|
| **Higher-risk Sub-contractor** | means a Sub-contractor that Handles Authority Data, where that data includes either:<br>(e) the Personal Data of 1000 or more individuals in aggregate during the period between the first Operational Service Commencement Date and the date on which this Contract terminates in accordance with clause 4.1.24.1(b); or<br>(a) any part of that Personal Data includes any of the following:<br>(i) financial information (including any tax and/or welfare information) relating to any person;<br>(ii) any information relating to actual or alleged criminal offences (including criminal records);<br>(iii) any information relating to children and/or vulnerable persons;<br>(iv) any information relating to social care;<br>(v) any information relating to a person's current or past employment; or<br>(vi) Special Category Personal Data; or<br>(b) the Authority in its discretion, designates a Sub-contractor as a Higher-risk Subc-ontractor:<br>(i) in any procurement document related to this Contract; or<br>(ii) during the Term. |
| **HMG Baseline Personnel Security Standard** | means the employment controls applied to any individual member of the Supplier Personnel that performs any activity relating to the provision or management of the Services, as set out in "HMG Baseline Personnel Standard", Version 7.0, June 2024 (https://www.gov.uk/government/publications/government-baseline-personnel-security-standard), as that document is updated from time to time. |
| **Independent Security Adviser** | means the independent and appropriately qualified and experienced security architect or expert appointed under Paragraph 19. |
| **ISO Certification** | means either of the following certifications when issued by a UKAS-recognised Certification Body:<br>(a) ISO/IEC27001:2013, where the certification was obtained before November 2022, but only until November 2025; and<br>(b) ISO/IEC27001:2022 in all other cases. |
| **IT Health Check** | means testing of the Supplier Information Management System by a CHECK Service Provider. |

| | |
|---|---|
| **Key Sub-contractor Default** | has the meaning set out in Paragraph 10.5. |
| **Medium-risk Sub-contractor** | means a Sub-contractor that Handles Authority Data, [where that data<br>(a) includes the Personal Data of between 100 and 999 individuals (inclusive) in the period between the first Operational Service Commencement Date and the date on which this Contract terminates in accordance with clause 4.1.24.1(b); and<br>(b) does not include Special Category Personal Data]. |
| **Modules Register** | means the register of Third--party Software Modules required by Paragraph 7.3 of the Security Requirements. |
| **NCSC** | means the National Cyber Security Centre or any replacement or successor body carrying out the same function. |
| **NCSC Cloud Security Principles** | means 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** | means 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** | means 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 . |
| **NCSC Secure Design Principles** | means 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** | means the Open Web Application Security Project Foundation. |
| **OWASP Secure Coding Practice** | means 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** | means 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** | means a user with system administration access to the Supplier Information Management System, or substantially similar access privileges. |
| **Prohibited Activity** | means the storage, access or Handling of Authority Data prohibited by a Prohibition Notice. |
| **Prohibition Notice** | means a notice issued under Paragraph 1.11 of the Security Requirements. |

| | |
|---|---|
| **Protective Monitoring System** | means the system implemented by the Supplier and its Sub-contractors under Paragraph 14.1 of the Security Requirements to monitor and analyse access to and use of the Supplier Information Management System, the Development Environment, the Authority Data and the Code. |
| **RAP Trigger** | means the occurrence of one of the events set out in Paragraph 18.1. |
| **Register of Sites, Support Locations and Third-party Tools.** | means the part of the Security Management Plan setting out, in respect of Sites, Support Locations and Third-party Tools:<br>(a) the Sites, Support Locations and Third-party Tools that the Supplier will use to Handle Authority Data or provide the Services;<br>(b) the nature of the activity performed at the Site or Support Location or by the Third--party Tool in respect of the Authority Data;<br>(c) in respect of each entity providing a Site, Support Location or Third-party Tool, its:<br>(i) full legal name;<br>(ii) trading name (if any)<br>(iii) country of registration;<br>(iv) registration number (if applicable); and<br>(v) registered address. |
| **Relevant Activities** | means those activities specified in Paragraph 1.1 of the Security Requirements. |
| **Relevant Certifications** | means:<br>(a) in the case of the Supplier, any SIMS Sub-contractor and any Key Sub-contractor:<br>(i) either:<br>(A) an ISO Certification in respect of the Supplier Information Management System; or<br>(B) where the Supplier Information Management System is included within the scope of a wider ISO Certification, that ISO Certification; and<br>(ii) Cyber Essentials Plus;<br>(b) In the case of any Higher-risk Sub-contractor, either:<br>(i) an ISO Certification in respect of that part of the Supplier Information Management System provided by the Higher-risk Sub-contractor;<br>(ii) where the 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 |

| | |
|---|---|
| | (iii) Cyber Essentials Plus; and<br><br>(c) in the case of any Medium-risk Sub-contractors, means Cyber Essentials.<br><br>(or equivalent certifications). |
| **Relevant Convictions** | means any previous or pending prosecution, conviction or caution (excluding any spent conviction under the Rehabilitation of Offenders Act 1974) relating to offences involving dishonesty, terrorism, immigration, firearms, fraud, forgery, tax evasion, offences against people (including sexual offences), or any other offences relevant to Services as the Authority may specify. |
| **Remediation Action Plan** | means 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** | means a location other than a Supplier's or a Sub-contractor's Site. |
| **Remote Working** | means the provision or management of the Services by Supplier Personnel 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 the Security Requirements and forming part of the Security Management Plan under which Supplier Personnel are permitted to undertake Remote Working. |
| **Required Changes Register** | means the register recording each of the changes that the Supplier proposes to the Supplier Information Management System or the Security Management Plan together with:<br><br>(a) the details of any approval of the change provided by the Authority, including any conditions or limitations on that approval; and<br><br>(b) the date:<br><br>(i) the date by which the change it to be implemented; and<br><br>(ii) the date on which the change was implemented. |
| **Residual Risk Statement** | means a notice issued by the Authority that<br><br>(a) sets out the information risks associated with using the Supplier Information Management System; and<br><br>(b) confirms that the Authority:<br><br>(i) is satisfied that the identified risks have been adequately and appropriately addressed; and<br><br>(ii) that the residual risks are understood and accepted by the Authority. |
| **Risk Management Approval Statement** | the statement issued by the Authority under Paragraph **Error! Reference source not found.**16.2 following the Authority's review of the Security Management Plan. |

| | |
|---|---|
| **Secure by Design Principles** | means 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** | means 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(a) of Appendix 1 (*Security Requirements*). |
| **Security Controls** | means 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** | means 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** | mean the security requirements in Appendix 1 to this Schedule 5 (*Security Management*). |
| **Security Requirements for Development** | means the security requirement Appendix 2 to this Schedule 5 (*Security Management*). |
| **Security Test** | means:<br>(a) an IT Health Check; or<br>(b) a Supplier Security Test. |
| **Security Working Group** | means the Board established under Paragraph 8 or Schedule 21 (Governance), as applicable. |
| **SIMS Sub-contractor** | means a Sub-contractor designated by the Authority that provides or operates the whole, or a substantial part, of the Supplier Information Management System. |
| **SMP Sub-contractor** | means a Sub-contractor with significant market power, such that:<br>(a) they will not contract other than on their own contractual terms; and<br>(b) either:<br>(i) there are no other substitutable suppliers of the particular services other than SMP Sub-contractors; or<br>(ii) the Sub-contractor concerned has an effective monopoly on the provision of the Services. |
| **Statement of Information Risk Appetite** | means the statement provided by the Authority under Paragraph 14.1 setting out:<br>(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 Authority Data. |
| **Sub-contractor** | means, for the purposes of this Schedule 5 (*Security Management*) only, any individual or entity that:<br>(a) forms part of the supply chain of the Supplier; and<br>(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 Authority Data.<br>and this definition shall apply to this Schedule 5 in place of the definition of Sub-Contractor in Schedule 1 *(Definitions)*. |
| **Sub-contractor Personnel** | means:<br>(a) any individual engaged, directly or indirectly, or employed, by any Sub-contractor; and<br>(b) engaged in or likely to be engaged in:<br>(i) the performance or management of the Services;<br>(ii) or the provision of facilities or services that are necessary for the provision of the Services. |
| **Sub-contractors' Systems** | means the information and communications technology system used by a Sub-contractor in implementing and performing the Services, including:<br>(a) the Software;<br>(b) the Supplier Equipment;<br>(c) configuration and management utilities;<br>(d) calibration and testing tools;<br>(e) and related cabling; but<br>does not include the Authority System. |
| **Supplier Information Management System** | means<br>(f) the Supplier System;<br>(g) the Sites;<br>(h) any part of the Authority System the Supplier or any Sub-contractor will use to Process Authority Data, or provide the Services; and<br>(i) the associated information management system, including all relevant:<br>(i) organisational structure diagrams,<br>(ii) controls,<br>(iii) policies,<br>(iv) practices,<br>(v) procedures, |

| | |
|---|---|
| | (vi) processes; and<br><br>(vii) resources,<br><br>as determined by the Supplier after consultation with the Authority under Paragraph 11. |
| **Support Location** | means a place or facility where or from which individuals may access or Handle the Code or the Authority Data. |
| **Support Register** | means the register of all hardware and software used to provide the Services produced and maintained in accordance with Paragraph 5 of the Security Requirements. |
| **Third-party Software Module** | means any module, library or framework that:<br>(a) is not produced by the Supplier or a Sub-contractor as part of the Development Activity; and<br>(b) either:<br>(i) forms, or will form, part of the Code; or<br>(ii) is, or will be, accessed by the Developed System during its operation. |
| **Third-party Tool** | means any Software used by the Supplier by which the Code or the Authority Data is accessed, analysed or modified or some form of operation is performed on it. |
| **UKAS** | means the United Kingdom Accreditation Service. |
| **UKAS-recognised Certification Body** | means:<br>(a) an organisation accredited by UKAS to provide certification of ISO/IEC27001:2013 and/or ISO/IEC27001:2022; or<br>(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. |
| **Wider Information Management System** | means<br>(a) any:<br>(i) information assets,<br>(ii) IT systems,<br>(iii) IT services; or Sites<br>that the Supplier or any Sub-contractor will use to Handle, or support the Handling of, Authority Data and provide, manage or support the provision of, the Services; and<br>(b) the associated information management system, including all relevant:<br>(i) organisational structure diagrams,<br>(ii) controls, |

| | |
|---|---|
| | (iii) policies,<br>(iv) practices,<br>(v) procedures,<br>(vi) processes; and<br>(vii) resources. |

## 3 Introduction

This Schedule 5 (*Security Management*) sets out:

3.1 the Authority's decision on where the Supplier may:

(a) store, access or Handle Authority Data;

(b) undertake the Development Activity;

(c) host the Development Environment; and

(d) locate Support Locations,

(in Paragraph 1);

3.2 the principles of security that apply to this Contract (in Paragraph 4);

3.3 the requirement to obtain a Risk Management Approval Statement (in Paragraphs 6 and 16);

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 Schedule [17] (*Governance*) (in Paragraph 8);

3.6 access to personnel (in Paragraph 9);

3.7 obligations in relation to Sub-contractors (in Paragraph 10);

3.8 the responsibility of the Supplier to determine the Supplier Information Management System (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 (in Paragraphs 14, 15 and 16);

3.11 the granting by the Authority of approval for the Supplier to commence:

(a) the provision of Operational Services; and/or

(b) Handling Authority Data (in Paragraph 16);

3.12 the management of changes to the Supplier Information Management System (in Paragraph 17); and

3.13 the Authority's additional remedies for breach of this Schedule 5 (*Security Management*), including:

(a) the requirement for Remediation Action Plans (in Paragraph 18);

(b) the appointment of Independent Security Advisers (in Paragraph 19); and

(c) the withholding of Charges by the Authority (in Paragraph 20).

## 4 Principles of security

4.1 The Supplier acknowledges that the Authority places great emphasis on the confidentiality, integrity and availability of the Authority Data and, consequently, on the security of:

(a) the Authority System;

(b) the Supplier System;

(c) the Sites;

(d) the Services; and

(e) 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 any approvals or agreements provided by the Authority under this Schedule 5 (*Security Management*), the Supplier remains responsible for:

(a) the security, confidentiality, integrity and availability of the Authority Data when that Authority Data is under the control of the Supplier or any of its Sub-contractors; and

(b) the security of the Supplier Information Management System.

## 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 Authority:

(a) comply with the Security Requirements in Appendix 1;

(b) where the relevant option in Paragraph 1 is selected, comply with the Security Requirements for Development in Appendix 2;

(c) where the relevant option in Paragraph 1 is selected, comply with the Authority Security Policies; and

(d) ensure that Sub-contractors comply with:

(i) all Security Requirements in Appendix 1;

(ii) where the relevant option in Paragraph 1 is selected, all Security Requirements for Development in Appendix 2; and

(iii) where the relevant option in Paragraph 1 is selected, all Authority Security Policies,

that apply to the activities that the Sub-contractor performs under its Sub-contract, unless:

(iv) Paragraph 5.4 applies; or

(v) the table in Appendix 4 limits the Security Requirements or Security Requirements for Development that apply to a Sub-contractor.

5.3 Where the Authority selects the option in Paragraph 1 requiring the Supplier to comply with the Authority Security Policies, if there is an inconsistency between the Authority Security Requirements and the requirement of this Schedule 5 (*Security Management*), then the requirements of this Schedule 5 (*Security Management*) will prevail to the extent of that inconsistency.

5.4 Where a Sub-contractor is a SMP Sub-contractor, the Supplier shall:

(a) use reasonable endeavours to ensure that the SMP Sub-contractor complies with all obligations that this Schedule 5 (*Security Management*) imposes on Sub-contractors, including the Security Requirements;

(b) document the differences between those obligations and the obligations that the SMP Sub-contractor is prepared to accept in sufficient detail to allow the Authority to form an informed view of the risks concerned;

(c) take such steps as the Authority may require to mitigate those risks.

## 6 Authority to proceed

Notwithstanding anything in this Contract, the Supplier may not:

6.1 commence the provision of any Operational Services; or

6.2 Handle any Authority 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 the Security Requirements; and

6.5 the Authority has issued a Risk Management Approval Statement under Paragraph 16.2.

## 7 Supplier confirmation

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

(a) the Supplier has in the previous year carried out all tests and has in place all procedures required in relation to security matters required by this Contract;

(b) subject to Paragraph 7.2:

(i) it has fully complied with all requirements of this Schedule 5 (*Security Management*); and

(ii) all Sub-contractors have complied with the requirements of this Schedule 5 (*Security Management*) with which the Supplier is required to ensure they comply;

(c) the Supplier considers that its security and risk mitigation procedures remain effective.

7.2 Where the Authority has, in respect of the period covered by the confirmation provided under Paragraph 7.1 agreed in writing that the Supplier need not, or need only partially, comply within any requirement of this Schedule 5 (*Security Management*):

(a) the confirmation must include details of the Authority's agreement; and

(b) confirm that the Supplier has fully complied with that modified requirement.

7.3 The Supplier must:

(a) keep and maintain a register setting out all agreements referred to in Paragraph 7.2; and

(b) provide a copy of that register to the Authority on request.

## 8 Governance, information sharing and co-operation

**Governance**

8.1 Paragraphs 8.1 to 8.8 apply where a Security Working Group, or Board (as that term is defined in Schedule 17 (*Governance*)), with a similar remit, is not provided for otherwise in this Contract.

8.2 The Authority must establish a Security Working Group on which both the Authority and the Supplier are represented.

8.3 The notice or other document establishing the Security Working Group must set out:

(a) the Authority members;

(b) the Supplier members;

(c) the chairperson of the Security Working Group;

(d) the date of the first meeting;

(e) the frequency of meetings; and

(f) the location of meetings

8.4 The Security Working Group has oversight of all matters relating to the security of the Authority Data and the Supplier Information Management System.

8.5 The Security Working Group meets:

(a) at least once every three months; and

(b) additionally when required by the Authority.

8.6 The Supplier must ensure that the Supplier Personnel attending each meeting of the Security Working Group:

(a) have sufficient knowledge and experience to contribute to the discussion of the matters on the agenda for the meeting;

(b) 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

(c) where relevant to the matters on the agenda for the meeting, include representatives of relevant Sub-contractors.

8.7 Any decisions, recommendations or advice of the Security Working Group:

(a) are binding on the Supplier, unless:

(i) the Authority agrees otherwise; or

(ii) the decision, recommendation or advice of the Security Working Group imposes on the Supplier more onerous requirements than those provided for in this Schedule 5 (*Security Management*); and

(b) do not limit or modify the Supplier's responsibilities under this Schedule 5 (*Security Management*).

8.8 Appendix 3 applies to the Security Working Group.

## 9 Personnel

9.1 The Supplier must ensure that at all times it maintains within the Supplier Personnel sufficient numbers of qualified, skilled security professionals to ensure the Supplier complies with the requirements of this Schedule 5 (*Security Management*).

9.2 The Supplier must appoint:

(a) a senior individual within its organisation with accountability for managing security risks and the Supplier's implementation of the requirements of this Schedule 5 (*Security Management*); and

(b) 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:

(a) must have sufficient experience, knowledge and authority to undertake their roles effectively; and

(b) are to be designated as Key Personnel and treated for the purposes of this Contract as Key Personnel, whether or not they are otherwise designated as such;

9.4 The Supplier must review, and if necessary replace, the individuals appointed under Paragraph 9.2 if required to do so by the Authority.

9.5 To facilitate:

(a) the Authority's oversight of the Supplier Information Management System; and

(b) 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:

(c) the Supplier shall provide access to the Supplier Personnel responsible for information assurance; and

(d) the Authority shall provide access to its personnel 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 Sub-contractor.

10.3 In addition to the obligations imposed by this Contract on Key Sub-contractors, the Supplier must ensure that the Key Subcontract with each SIMS Sub-contractor contains obligations no less onerous on the Key Sub-contractor than those imposed on the Supplier under this Schedule 5 (*Security Management*).

**Sub-contractors**

10.4 The Supplier must, before entering into a binding Sub-contract with any Sub-contractor:

(a) 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 5 (*Security Management*) requires the Supplier ensure that the proposed Sub-contractor performs;

(b) keeps adequate records of the due diligence it has undertaken in respect of the proposed Sub-contractors; and

(c) provides those records to the Authority on request.

**Key Sub-contractor Default**

10.5 Where the Supplier becomes aware of an actual or suspected failure by a Key Sub-contractor to comply with any obligation in this Schedule 5 (*Security Management*) with which the Supplier is, by virtue of Paragraph 5.2(b), required to ensure the Key Sub-contractor complies (**Key Sub-contractor Default**), the Supplier must:

(a) as soon as reasonably practicable and in any event within two Working days of becoming aware of the Key Sub-contractor Default notify the Authority setting out the actual or anticipated effect of the Key Sub-contractor Default; and

(b) unless the Authority waives the requirement, comply with the Remediation Action Plan process in Paragraph 18.

## 11 Supplier Information Management System

11.1 The Supplier must determine:

(a) the scope and component parts of the Supplier Information Management System; and

(b) the boundary between the Supplier Information Management System and the Wider Information Management System.

11.2 Before making its determination under Paragraph 11.1, the Supplier must consult with the Authority and in doing so must provide the Authority with such documentation and information that the Authority may require regarding the Wider Information Management System.

11.3 The Supplier shall reproduce its decision under Paragraph 11.1 as a diagram documenting the components and systems forming part of, and the boundary between, the Supplier Information Management System and the Wider Information Management System.

11.4 The diagram prepared under Paragraph 11.3 forms part of the Security Management Plan.

11.5 Any proposed change to:

(a) the component parts of the Supplier Information Management System; or

(b) the boundary between the Supplier Information Management System and the Wider Information Management System,

is:

(c) an Operational Change to which the Change Control Procedure applies;

(d) requires approval by the Authority under Paragraph 17; and

(e) the Authority may require the appointment of an Independent Security Adviser to advise on the proposed change.

## 12 Authority Data Handled using Supplier Information Management System

12.1 The Supplier acknowledges that the Supplier Information Management System:

(a) is intended only for the Handling of Authority Data that is classified as OFFICIAL; and

(b) is not intended for the Handling of Authority Data that is classified as SECRET or TOP SECRET,

in each case using the Government Security Classification Policy.

12.2 The Supplier must:

(a) not alter the classification of any Authority Data; and

(b) if it becomes aware that any Authority Data classified as SECRET or TOP SECRET is being Handled using the Supplier Information Management System:

(i) immediately inform the Authority; and

(ii) follow any instructions from the Authority concerning that Authority Data.

12.3 The Supplier must, and must ensure that Sub-contractors and Supplier Personnel, when Handling Authority Data, comply with:

(a) the Expected Behaviours; and

(b) the Security Controls.

12.4 Where there is a conflict between the Expected Behaviours or the Security Controls and this Schedule 5 (*Security Management*) the provisions of this Schedule 5 (*Security Management*) shall apply to the extent of any conflict.

## 13 Certification Requirements

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

(a) it; and

(b) any SIMS Sub-contractor, any Key Sub-contractor, any Higher-risk Sub-contractor and any Medium-risk Sub-contractor,

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

(c) in the case of the Supplier, any SIMS Sub-contractor and any Key Sub-contractor:

(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;

(or equivalent); and

(d) 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; or

(ii) 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

(iii) Cyber Essentials Plus; and

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

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

(a) the Relevant Certifications for it and any Sub-contractor; and

(b) 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:

(a) currently in effect;

(b) together cover at least the full scope of the Supplier Information Management System; and

(c) 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 Authority promptly, and in any event within three Working Days, after becoming aware that, in respect of it or any Sub-contractor:

(a) a Relevant Certification in respect of the Supplier Information Management System has been revoked or cancelled by the body that awarded it;

(b) a Relevant Certification in respect of the Supplier Information Management System has expired and has not been renewed by the Supplier;

(c) the Relevant Certifications together no longer apply to the full scope of the Supplier Information Management System; or

(d) 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 Authority of a Certification Default under Paragraph 13.4:

(a) 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 Authority setting out:

(i) full details of the Certification Default, including a root cause analysis;

(ii) the actual and anticipated effects of the Certification Default;

(iii) the steps the Supplier and any Sub-contractor to which the Certification Default relates will take to remedy the Certification Default;

(b) the Authority must notify the Supplier as soon as reasonably practicable whether it accepts or rejects the Certification Rectification Plan;

(c) if the Authority 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(b) will apply to the re-submitted plan;

(d) the rejection by the Authority of a revised Certification Rectification Plan is a material Default of this Contract;

(e) if the Authority accepts the Certification Rectification Plan, the Supplier must start work immediately on the plan.

## 14 Security Management Plan

**Purpose of Security Management Plan**

14.1 The Authority 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:

(a) comply with the requirements set out in this Schedule 5 (*Security Management*) and the Contract in order to ensure the security of the Authority Data and the Supplier Information Management System; and

(b) 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:

(a) the Security Management Plan accurately represents the Supplier Information Management System;

(b) the Supplier Information Management System will meet the requirements of this Schedule 5 (*Security Management*) and the Statement of Information Risk Appetite (where one has been provided); and

(c) 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 Authority:

(a) by the date specified in the Detailed Implementation Plan; or

(b) if no such date is specified, in sufficient time to allow for the Authority review and approve the Security Management Plan before the first Operational Service Commencement Date.

14.5 If Paragraph 14.4(b) applies, and any delay resulting from the Authority's review and approval of the Security Management Plan (including any additional activity required by the Supplier to ensure the Security Management Plan complies with Paragraph 14.3) causes or contributes to Supplier Non-Performance under clause 29.1 that delay is not an Authority Cause and the Supplier shall not be entitled to any relief or compensation under clause 29.

**Contents of Security Management Plan**

14.6 The Security Management Plan must include:

(a) a formal information risk assessment of, and a risk treatment plan for, the Supplier Information Management System;

(b) a completed statement of applicability under the relevant ISO Certification for the Supplier Information Management System;

(c) 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 Authority Data;

(d) unless such requirement is waived by the Authority, an assessment of the Supplier Information Management System against the table in Appendix 6 (*Secure by Design Principles Evaluation Table*);

(e) unless such requirement is waived by the Authority, the controls the Supplier will implement in respect of the Services and all processes associated with the delivery of the Services, including:

(i) the Supplier System;

(ii) the Sites; and

(iii) the Authority System (to the extent that it is under the control of the Supplier); and

(iv) any IT, Information and data (including the Confidential Information of the Authority and the Authority Data) to the extent used by the Authority or the Supplier:

(A) in connection with this Contract or

(B) in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Services;

(f) the Required Changes Register;

(g) evidence that the Supplier and each Sub-contractor (so far as those requirements apply) is compliant with:

(i) the Certification Requirements;

(ii) the Security Requirements; and

(iii) where the relevant option in Paragraph 1 is selected, the Security Requirements for Development;

(h) the diagram documenting the Supplier Information Management System, the Wider Information Management System and the boundary between them (created under Paragraph 11).

(i) an assessment of the Supplier Information Management System against the requirements of this Schedule 5 (*Security Management*), including the Security Requirements and, where the relevant option in Paragraph 1 is selected, the Security Requirements for Development (where applicable);

(j) the process the Supplier will implement immediately after it becomes aware of a Breach of Security to restore normal operations as quickly as possible, minimising any adverse impact on the Authority Data, the Authority, the Services and/or users of the Services; and

(k) the following information, so far as is applicable, in respect of each Sub-contractor:

(i) the Sub-contractor's:

(A) legal name;

(B) trading name (if any); and

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

(ii) the Relevant Certifications held by the Sub-contractor;

(iii) the Sites used by the Sub-contractor;

(iv) the Services provided, or contributed to, by the Sub-contractor;

(v) the access the Sub-contractor has to the Supplier Information Management System;

(vi) the Authority Data Handled by the Sub-contractor;

(vii) the Handling that the Sub-contractor will undertake in respect of the Authority Data; and

(viii) the measures the Sub-contractor has in place to comply with the requirements of this Schedule 5 (*Security Management*); and

(ix) the due diligence the Supplier has taken to assess that compliance;

(l) the Register of Sites, Support Locations and Third-party Tools;

(m) the Modules Register;

(n) the Support Register;

(o) the Backup and Recovery Plan;

(p) the Remote Working Policy (where the Supplier or a Sub-contractor proposes to allow Supplier Personnel to work from a Remote Location); and

(q) details of the protective monitoring that the Supplier will undertake in accordance with Paragraph 14 of the Security Requirements, including:

(i) the additional audit and monitoring the Supplier will undertake of the Supplier Information Management System; and

(ii) the retention periods for audit records and event logs.

## 15 Monitoring and updating Security Management Plan

**Updating Security Management Plan**

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

**Monitoring**

15.2 The Supplier, where it plans to undertake, or after becoming aware of, any of the following:

(a) a significant change to the components or architecture of the Supplier Information Management System;

(b) a significant change in the boundary between the Supplier Information Management System and the Wider Information Management System

(c) a significant change in the operation of the Supplier Information Management System;

(d) the replacement of an existing, or the appointment of a new:

(i) SIMS Sub-contractor; or

(ii) Sub-contractor that Handles Authority Data;

(e) a significant change in the quantity of Personal Data held within the Service; and/or

(f) wofhere the Supplier or a Sub-contractor has previously Handled Authority Data that is Personal Data, other than Special Category Personal Data, it proposes to start to Handle Authority Data that is Special Category Personal Data under this Contract;

must:

(g) within two Working Days notify the Authority; and

(h) within ten Working Days, or such other timescale as may be agreed with the Authority:

(i) update the Required Changes Register and any other affected parts of the Security Management Plan; and

(ii) provide the Authority with a copy of those documents for review and approval.

15.3 Paragraph 15.2 applies in addition to, and not in substitution of, the Parties obligations to comply with the Change Control Procedure for any Contract Change or Operational Change.

15.4 Any proposed change under Paragraph 15.2(a), 15.2(b) or 15.2(f) constitutes a Contract Change to which the Change Control Procedure applies.

## 16 Review and approval of updated Security Management Plan

16.1 Where the Supplier has prepared or updated the Security Management Plan the Authority may review the plan and to do so may request such further information as the Authority considers necessary or desirable.

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

(a) where satisfied that the:

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

(ii) that the residual risks are:

(A) either:

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

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

(B) understood and accepted by the Authority; and

(C) recorded in the Residual Risk Statement;

a Risk Management Approval Statement; or

(b) where the Authority reasonably considers that:

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

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

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

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

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

## 17 Changes to the Supplier Information Management System

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

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

(b) a significant change in the operation or management of the Supplier Information Management System; or

(c) the appointment of a new, or the replacement of an existing:

(i) SIMS Sub-contractor; or

(ii) Sub-contractor that Handles Authority Data.

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

(a) update the Required Changes Register;

(b) prepare a proposal for the Authority setting out:

(i) details of the proposed changes to the Supplier Information Management System;

(ii) an assessment of the security implications of the proposed change;

(iii) a risk assessment of the proposed change; and

(iv) any proposed changes to the Security Management Plan; and

(c) provide that paper to the Authority no later than 30 Working Days before the date on which it will consider the proposed changes.

17.3 The Authority:

(a) may request such further information as the Authority considers necessary or desirable;

(b) must provide its decision within 20 Working Days of the later of:

(i) the date on which it receives the proposal; or

(ii) the date on which it receives any requested further information;

(c) must not:

(i) unreasonably refuse any proposal by the Supplier; and

(ii) must not make any approval subject to unreasonable conditions.

17.4 If the Authority does not provide a decision within the period specified in Paragraph 17.3(b), the proposal shall be deemed to have been accepted.

**Implementation of changes**

17.5 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.

17.6 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:

(a) that failure is a material Default; and

(b) the Supplier shall:

(i) immediately cease using the Supplier Information Management System to Handle Authority Data either:

(A) until the Default is remedied, or

(B) unless directed otherwise by the Authority in writing and then only in accordance with the Authority's written directions; and

(ii) where such material Default is capable of remedy, remedy such material Default within the timescales set by the Authority (considering the security risks the material Default presents to the Services and/or the Supplier Information Management System).

## 18 Remediation Action Plan

**Preparation of Remediation Action Plan**

18.1 This Paragraph 18 applies when:

(a) Key Sub-contractor Default occurs;

(b) the Authority issues a Risk Management Rejection Notice; or

(c) 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**).

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

18.3 The draft Remediation Action Plan must, in respect of each issue raised by the RAP Trigger, set out:

(a) full details of that issue;

(b) the actual or anticipated effect of that issue;

(c) how the issue will be remedied;

(d) the date by which the issue will be remedied; and

(e) the tests that the Supplier proposes to perform to confirm that the issue has been remedied.

**Consideration of Remediation Action Plan**

18.4 The Supplier must

(a) provide the Authority with a copy of any Remediation Action Plan it prepares;

(b) have regard to any comments the Authority provides in respect of the Remediation Action Plan; and

(c) fully implement the Remediation Action Plan according to its terms.

**Implementing an approved Remediation Action Plan**

18.5 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.

18.6 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:

(a) provide the Authority with a full, unedited and unredacted copy of the test report;

(b) implement interim mitigation measures to vulnerabilities in the Information System known to be exploitable where a security patch is not immediately available;

(c) as far as practicable, remove or disable any extraneous interfaces, services or capabilities not needed for the provision of the Services within the timescales set out in the test report or such other timescales as may be agreed with the Authority.

## 19 Independent Security Adviser

19.1 The Authority may require the appointment of an Independent Security Adviser where:

(a) there is a proposed change to the Supplier Information Management System (see Paragraph 11.5);

(b) the Authority issues two or more Risk Management Rejection Notices (see Paragraph 16.2); or

(c) either:

(i) a Security Test report identifies more than ten vulnerabilities classified as either critical or high; or

(ii) the Authority rejected a revised draft Remediation Action Plan (see Paragraph 12.21 of Appendix 1).

19.2 Where the Authority requires the appointment of an Independent Security Adviser the Independent Security Adviser shall be:

(a) a person selected by the Supplier and approved by the Authority; or

(b) where

(i) the Authority does not approve the persons selected by the Supplier; or

(ii) the Supplier does not select any person within ten Working Days of the date of the notice requiring the Independent Security Adviser's appointment,

a person selected by the Authority.

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

(a) 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

(b) provide advice and recommendations on:

(i) steps the Supplier can reasonably take to improvement the security of the Supplier Information Management System; and

(ii) 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.

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

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

(b) gather any information the Independent Security Adviser considers relevant in the furtherance of their appointment;

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

(d) make recommendations to the Authority and/or the Supplier as to how the matters leading to their appointment might be mitigated or avoided in the future; and/or

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

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

(a) 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;

(b) 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;

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

(d) implement any recommendations (including additional security measures and/or controls) made by the Independent Security Adviser that have been approved by the Authority within the timescales given by the Independent Security Adviser; and

(e) not terminate the appointment of the Independent Security Adviser without the prior consent of the Authority (unless such consent has been unreasonably withheld).

19.6 The Supplier shall be responsible for:

(a) the costs of appointing, and the fees charged by, the Independent Security Adviser; and

(b) its own costs in connection with any action required by the Authority and/or the Independent Security Adviser.

19.7 If the Supplier or any relevant Sub-contractor:

(a) fails to perform any of the steps required by the Authority in the notice appointing the Independent Security Adviser; and/or

(b) is in Default of any of its obligations under this Paragraph 19,

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

## 20 Withholding of Charges

20.1 The Authority may withhold some or all of the Charges in accordance with the provisions of this Paragraph 20 where:

(a) the Supplier is in material Default of any of its obligations under this Schedule 5 (*Security Management*); or

(b) any of the following matters occurs (where those matters arise from a Default by the Supplier of its obligations under this Schedule 5 (*Security Management*)):

(i) a Notifiable Default;

(ii) an Intervention Cause; or

(iii) a Step-In Trigger Event.

20.2 The Authority may withhold an amount of the Charges that it considers sufficient, in its sole discretion, to incentivise the Supplier to perform the obligations it has Defaulted upon.

20.3 Before withholding any Charges under Paragraph 20.1 the Authority must

(a) provide written notice to the Supplier setting out:

(i) the Default in respect of which the Authority has decided to withhold some or all of the Charges;

(ii) the amount of the Charges that the Authority will withhold;

(iii) the steps the Supplier must take to remedy the Default;

(iv) the date by which the Supplier must remedy the Default;

(v) the invoice in respect of which the Authority will withhold the Charges; and

(b) consider any representations that the Supplier may make concerning the Authority's decision.

20.4 Where the Supplier does not remedy the Default by the date specified in the notice given under Paragraph 20.3(a), the Authority may retain the withheld amount.

20.5 The Supplier acknowledges:

(a) the legitimate interest that the Authority has in ensuring the security of the Supplier Information Management System and the Authority Data and, as a consequence, the performance by the Supplier of its obligations under this Schedule 5 (*Security Management*); and

(b) that any Charges that are retained by the Authority are not out of all proportion to the Authority's legitimate interest, even where:

(i) the Authority has not suffered any Losses as a result of the Supplier's Default; or

(ii) the value of the Losses suffered by the Authority as a result of the Supplier's Default is lower than the amount of the Charges retained.

20.6 The Supplier may raise a Dispute under the Dispute Resolution Procedure with any decision by the Authority to:

(a) withhold any Charges under Paragraph 20.1; or

(b) retain any Charges under Paragraph 20.4.

20.7 Any Dispute raised by the Supplier does not prevent the Authority withholding Charges in respect of:

(a) the decision subject to the Dispute; or

(b) any other matter to which this Paragraph 20 applies.

20.8 Where any Dispute raised by the Supplier is resolved wholly or partially in its favour, the Authority must return such sums as are specified in any agreement or other document setting out the resolution of the Dispute.

20.9 The Authority's right to withhold or retain any amount under this Paragraph 20 are in addition to any other rights that the Authority may have under this Contract or in Law, including any right to claim damages for Losses it suffers arising from the Default.

## 21 Access to Authority System

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

# Appendix 1 Security Requirements

## 1 Location

**Location for Relevant Activities**

1.1 Unless otherwise agreed with the Authority, the Supplier must, and ensure that its Sub-contractors, at all times:

(a) provide the Services;

(b) undertake any activity supporting or managing:

(i) the Services;

(ii) the Supplier Information Management System; or

(iii) the Wider Information Management System;

(c) store, access or Handle Authority Data;

(d) undertake the Development Activity; and

(e) host the Wider Information Management System, including any Sites

(together, the **Relevant Activities**)

only in or from the geographic areas permitted by the Authority in Paragraph 1.

1.2 Where the Authority has not selected an option concerning location in Paragraph 1, the Supplier may only undertake the Relevant Activities in or from:

(a) the United Kingdom; or

(b) 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:

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

(b) that binding agreement includes obligations on the entity in relation to security management equivalent to those imposed on Sub-contractors in this Schedule 5 (*Security Management*);

(c) the Supplier or Sub-contractor has taken reasonable steps to assure itself that the entity complies with the binding agreement;

(d) the Supplier has provided the Authority with such information as the Authority requires concerning:

(i) the entity;

(ii) the arrangements with the entity; and

(iii) the entity's compliance with the binding agreement; and

(e) the Authority 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:

(a) it must provide the Authority with such information as the Authority requests concerning:

(i) the security controls in places at the relevant location or locations; and

(ii) where certain security controls are not, or only partially, implemented the reasons for this;

(b) the Authority may grant approval to use that location or those locations, and that approval may include conditions; and

(c) if the Authority does not grant permission to use that location or those locations, the Supplier must, within such period as the Authority may specify:

(i) cease to store, access or Handle Authority Data at that location or those locations;

(ii) sanitise, in accordance with instructions from the Authority, such equipment within the information and communications technology system used to store, access or Handle Authority Data at that location, or those locations, as the Authority may specify.

**Support Locations**

1.5 The Supplier must ensure that all Support Locations are located only in the geographic areas permitted by the Authority.

1.6 Where the Authority has not selected an option concerning location in Paragraph 1, the Supplier may only locate Support Locations in:

(a) the United Kingdom; or

(b) 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:

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

(b) the binding agreement includes obligations on the entity in relation to security management equivalent to those relating to Sub-contractors in this Schedule 5 (*Security Management*);

(c) the Supplier or Sub-contractor has taken reasonable steps to assure itself that the entity complies with the binding agreement;

(d) the Supplier has provided the Authority with such information as the Authority requires concerning:

(i) the entity;

(ii) the arrangements with the entity; and

(iii) the entity's compliance with the binding agreement; and

(e) the Authority 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:

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

(b) the Supplier has provided the Authority with such information as the Authority requires concerning:

(i) the arrangements with the provider of the Third-party Tool; and

(ii) the due diligence undertaken by the Supplier or Sub-contractor; and

(c) do not use a Third-party Tool in respect of which the Authority 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:

(a) 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

(b) a new Third-party Tool, or replace an existing Third -party Tool, without the permission of the Authority.

**Prohibited Activities**

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

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

(i) in any particular country or group of countries;

(ii) in or using facilities operated by any particular entity or group of entities; or

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

(b) use any specified Third-party Tool,

(a **Prohibition Notice**).

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

(a) undertakes any Prohibited Activities;

(b) operates any Support Locations; or

(c) 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:

(a) 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 Authority Data;

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

(c) the physical security risk assessment and site security plan for each Secure Location:

(i) considers whether different areas of the Secure Location require different security measures based on the functions of each area;

(ii) adopts a layered approach to physical security;

(iii) has sections dealing with the following matters:

(A) the perimeter of the Secure Location;

(B) the building fabric;

(C) security guarding;

(D) visitor and people management;

(E) server and communications rooms;

(F) protection of sensitive data;

(G) closed circuit television;

(H) automated access and control systems;

(I) intruder detection; and

(J) security control rooms.

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

# 3 Vetting, Training and Staff Access

**Vetting before performing or managing Services**

3.1 The Supplier must not engage Supplier Personnel, and must ensure that Sub-contractors do not engage Sub-contractor Personnel in:

(a) any activity relating to the provision or management of the Services; or

(b) any activity that allows or requires the Handling of Authority Data,

unless:

(c) that individual has passed the security checks listed in Paragraph 3.2; or

(d) the Authority 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:

(a) The checks required for the HMG Baseline Personnel Security Standard (BPSS) to verify:

(i) the individual's identity;

(ii) 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;

(iii) the individual's previous employment history; and

(iv) that the individual has no Relevant Convictions;

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

(c) such other checks for the Supplier Personnel of Sub-contractors as the Authority 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:

(a) as soon as practicable, and in any event within 20 Working Days of becoming aware of the issue, notify the Authority;

(b) provide such information relating to the Sub-contractor, its vetting processes and the roles the affected Sub-contractor Personnel will perform as the Authority reasonably requires; and

(c) comply, at the Supplier's cost, with all directions the Authority may provide concerning the vetting of the affected Sub-contractor Personnel and the management of the Sub-contractor.

**Annual training**

3.4 The Supplier must ensure, and ensure that Sub-contractors ensure, that all Supplier Personnel, complete and pass security training at least once every calendar year that covers:

(a) general training concerning security and data handling;

(b) Phishing, including the dangers from ransomware and other malware; and

(c) the Secure by Design Principles.

**Staff access**

3.5 The Supplier must ensure, and ensure that Sub-contractors ensure, that individual Supplier Personnel can access only the Authority 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 Personnel no longer require access to the Authority Data or any part of the Authority Data, their access to the Authority Data or that part of the Authority Data is revoked immediately when their requirement to access Authority Data ceases.

3.7 Where requested by the Authority, the Supplier must remove, and must ensure that Sub-contractors remove, an individual Supplier Personnel's access to the Authority Data, or part of that Authority Data specified by the Authority, 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:

(a) unless in writing by the Authority, Privileged Users do not undertake Remote Working;

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

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

(a) prepare and have approved by the Authority the Remote Working Policy in accordance with this Paragraph;

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

(c) ensure that Supplier Personnel undertake Remote Working only in accordance with the Remote Working Policy;

(d) may not permit any Supplier Personnel of the Supplier or any Sub-contractor to undertake Remote Working until the Remote Working Policy is approved by the Authority.

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

(a) restricting or prohibiting Supplier Personnel from printing documents in any Remote Location;

(b) restricting or prohibiting Supplier Personnel from downloading any Authority Data to any End-user Device other than an End User Device that:

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

(ii) complies with the requirements set out in Paragraph 4 (*End-user Devices*);

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

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

(e) for each different category of Supplier Personnel subject to the proposed Remote Working Policy:

(i) the types and volumes of Authority Data that the Supplier Personnel can Handle in a Remote Location and the Handling that those Supplier Personnel will undertake;

(ii) any identified security risks arising from the proposed Handling in a Remote Location;

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

(iv) the residual risk levels following the implementation of those mitigations, controls and measures;

(v) when the Supplier or Sub-contractor (as applicable) will implement the proposed mitigations, controls and measures; and

(vi) the business rules with which the Supplier Personnel must comply; and

(f) how the Supplier or the Subcontractor (as applicable) will:

(i) communicate the Remote Working Policy and business rules to Supplier Personnel; and

(ii) enforce the Remote Working Plan and business rules.

3.11 The Supplier may submit a proposed Remote Working Policy to the Authority for consideration at any time.

3.12 The Authority must, within 20 Working Days of the submission of a proposed Remote Working Plan, either:

(a) 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;

(b) reject the proposed Remote Working Policy, in which case:

(i) the Authority may set out any changes to the proposed Remote Working Policy the Authority requires to make the plan capable of approval; and

(ii) the Supplier may:

(A) revise the proposed Remote Working Plan; and

(B) re-submit the proposed Remote Working Plan to the Authority 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 Authority Data or Code is stored or Handled in accordance the following requirements:

(a) the operating system and any applications that store, Handle or have access to Authority 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;

(b) users must authenticate before gaining access;

(c) all Authority Data and Code must be encrypted using an encryption tool agreed to by the Authority;

(d) 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;

(e) 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 Authority Data and Code to ensure the security of that Authority Data and Code;

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

(g) 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 this Contract.

4.3 Where there is any conflict between the requirements of this Schedule 5 (*Security Management*) and the requirements of the NCSC Device Guidance, the requirements of this Schedule 5 (*Security Management*) take precedence.

## 5 Hardware and software support

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

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

(b) where there are any recognised security vulnerabilities, either:

(i) remedy vulnerabilities; or

(ii) 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:

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

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

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

5.5 The Supplier must:

(a) review and update the Support Register:

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

(ii) 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;

(iii) within ten Working Days of introducing new software, or removing existing software, from the Supplier Information Management System; and

(iv) at least once every 12 months;

(b) provide the Authority with a copy of the Support Register:

(i) whenever it updates the Support Register; and

(ii) otherwise when the Authority requests.

5.6 Where any element of the Supplier Information Management System consists of COTS Software, the Supplier shall ensure:

(a) those elements are always in mainstream or extended security support from the relevant vendor; and

(b) 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:

(a) regular firmware updates to the hardware; and

(b) 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 Authority Data, the Supplier must agree with the Authority the encryption methods that it and any Sub-contractors that Handle Authority Data will use to comply with this Paragraph 6.

**6.2** Where this Paragraph 6 requires Authority Data to be encrypted, the Supplier must use, and ensure that Subcontractors use, the methods agreed by the Authority under Paragraph 6.1.

6.3 Unless Paragraph 6.4 applies, the Supplier must ensure, and must ensure that all Sub-contractors ensure, that Authority Data is encrypted:

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

(b) when transmitted.

6.4 Where the Supplier, or a Sub-contractor, cannot encrypt Authority Data as required by Paragraph 6.2, the Supplier must:

(a) immediately inform the Authority of the subset or subsets of Authority Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;

(b) provide details of the protective measures the Supplier or Sub-contractor (as applicable) proposes to take to provide equivalent protection to the Authority as encryption;

(c) provide the Authority with such additional information relating to the information provided under Paragraphs (a) and (b) as the Authority may require.

6.5 The Authority, the Supplier and, where the Authority requires, any relevant Sub-contractor shall meet to agree appropriate protective measures for the unencrypted Authority Data.

6.6 Where the Authority and Supplier reach agreement, the Supplier must update the Security Management Plan to include:

(a) the subset or subsets of Authority Data not encrypted and the circumstances in which that will occur;

(b) the protective measure that the Supplier and/or Sub-contractor will put in place in respect of the unencrypted Authority Data.

6.7 Where the Authority and Supplier do not reach agreement within 40 Working Days of the date on which the Supplier first notified the Authority that it could not encrypt certain Authority

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 Authority Data

**Backups and recovery of Authority Data**

7.1 The Supplier must backup and recover the Authority Data in accordance with the Backup and Recovery Plan to ensure the recovery point objective and recovery time objective in Paragraph 7.3(a).

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 5 (*Security Management*) and the Security Requirements apply.

**Backup and Recovery Plan**

7.3 Unless otherwise required by the Authority, the Backup and Recovery Plan must provide for:

(a) in the case of a full or partial failure of the Supplier System or a Sub-contractor's System:

(i) a recovery time objective of 72 hours and

(ii) a recovery point objective of the contract Effective Date through to the date the full or partial failure occurred.

(b) a retention period of 5 years or the length of the contract term whichever is the shortest.

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:

(a) the backup location for Authority 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;

(b) there is sufficient storage volume for the amount of Authority Data to be backed up;

(c) all back-up media for Authority Data is used in accordance with the manufacturer's usage recommendations;

(d) newer backups of Authority Data do not overwrite existing backups made during the retention period specified in Paragraph 7.3(a)(ii);

(e) the backup system monitors backups of Authority Data to:

(i) identifies any backup failure; and

(ii) confirm the integrity of the Authority Data backed up;

(f) any backup failure is remedied promptly;

(g) the backup system monitors the recovery of Authority Data to:

(i) identify any recovery failure;

(ii) confirm the integrity of Authority Data recovered; and

(h) 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 Authority, it:

(a) supports transport layer security (**TLS**) version 1.2, or higher, for sending and receiving emails;

(b) supports TLS Reporting (**TLS-RPT**);

(c) is capable of implementing:

(i) domain -based message authentication, reporting and conformance (**DMARC**);

(ii) sender policy framework (**SPF**); and

(iii) domain keys identified mail (**DKIM**); and

(d) is capable of complying in all respects with any guidance concerning email security as issued or updated from time to time by:

(i) the UK Government (current version at https://www.gov.uk/guidance/set-up-government-email-services-securely; or

(ii) the NCSC (current version at https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing).

## 9 DNS

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

## 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:

(a) prevents the installation of the most common forms of Malicious Software in the Supplier Information Management System and the Development Environment;

(b) is configured to perform automatic software and definition updates;

(c) provides for all updates to the Anti-virus Software to be deployed within ten Working Days of the update's release by the vendor;

(d) performs regular scans of the Supplier Information Management System to check for and prevent the introduction of Malicious Software; and

(e) 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 Authority 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 Authority 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:

(a) seven days after the public release of patches for vulnerabilities classified as "critical";

(b) 30 days after the public release of patches for vulnerabilities classified as "important"; and

(c) 60 days after the public release of patches for vulnerabilities classified as "other".

11.2 The Supplier must:

(a) scan the Supplier Information Management System and the Development Environment at least once every month to identify any unpatched vulnerabilities; and

(b) 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:

(a) the National Vulnerability Database's vulnerability security ratings; or

(b) Microsoft's security bulletin severity rating system.

## 12 Security testing

**Responsibility for security testing**

12.1 The Supplier is solely responsible for:

(a) the costs of conducting any security testing required by this Paragraph 12; and

(b) the costs of implementing any findings, or remedying any vulnerabilities, identified in that security testing.

**Security tests by Supplier**

12.2 The Supplier must:

(a) before submitting the draft Security Management Plan to the Authority for a decision under Paragraph 14;

(b) at least once during each Contract Year; and

(c) when required to do so by the Authority;

undertake the following activities:

(d) conduct security testing of the Supplier Information Management System (**IT Health Check**) in accordance with Paragraph 12.8 to 12.10; and

(e) 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:

(a) any Remediation Action Plan;

(b) the ISO27001 Certification Requirements;

(c) the Security Management Plan; and

(d) the Authority, following a Breach of Security or a significant change, as assessed by the Authority, to the components or architecture of the Supplier Information Management System,

(each a **Supplier Security Test**).

12.4 The Supplier must:

(a) design and implement the Supplier Security Tests so as to minimise the impact on the delivery of the Services;

(b) agree the date, timing, content and conduct of such Supplier Security Tests in advance with the Authority.

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 Authority may send a representative to witness the conduct of the Supplier Security Tests.

12.7 The Supplier shall provide the Authority with a full, unedited and unredacted copy of the results of such Security Tests (in a form approved by the Authority in advance) as soon as practicable, and in any case within ten Working Days, after completion of each Supplier Security Test

**IT Health Checks**

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

(a) use only a CHECK Service Provider to perform the IT Health Check;

(b) ensure that the CHECK Service Provider uses a qualified CHECK Team Leader and CHECK Team Members to perform the IT Health Check;

(c) 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.

(d) promptly provide the Authority with such technical and other information relating to the Information Management System as the Authority requests;

(e) include within the scope of the IT Health Check such tests as the Authority requires;

(f) agree with the Authority 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 Authority.

12.10 Following completion of an IT Health Check, the Supplier must provide the Authority with a full, unedited and unredacted copy of the report relating to the IT Health Check without delay and in any event within ten Working Days of its receipt by the Supplier.

**Remedying vulnerabilities**

12.11 In addition to complying with Paragraphs 12.13 to 12.21, the Supplier must remedy:

(a) any vulnerabilities classified as critical in a Security Test report within five Working Days of becoming aware of the vulnerability and its classification;

(b) any vulnerabilities classified as high in a Security Test report within one month of becoming aware of the vulnerability and its classification; and

(c) 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 Authority immediately if it does not, or considers it will not be able to, remedy the vulnerabilities classified as critical, high or medium in a Security Test report within the time periods specified in Paragraph 12.11.

**Responding to a Security Test report**

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 Authority a draft plan addressing the vulnerabilities and findings (**Remediation Action Plan**).

12.14 Where the Authority has commissioned a root cause analysis under Paragraph 12.21, the Supplier shall ensure that the draft Remediation Action Plan addresses that analysis.

12.15 The draft Remediation Action Plan must, in respect of each vulnerability identified or finding made by the Security Test report:

(a) how the vulnerability or finding will be remedied;

(b) the date by which the vulnerability or finding will be remedied; and

(c) 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 Authority with such technical and other information relating to the Supplier Information Management System, the IT Health Check report or the draft Remediation Action Plan as the Authority requests.

12.17 The Authority may:

(a) 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:

(i) the Supplier shall within ten Working Days of the date on which the Authority rejected the draft Remediation Action Plan submit a revised draft Remediation Action Plan that takes into account the Authority's reasons; and

(ii) Paragraph 12.15 to 12.17 shall apply, with appropriate modifications, to the revised draft Remediation Action Plan;

(b) 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 Authority unreasonably:

(a) delays its approval; or

(b) rejects,

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

(c) arose directly from the Authority unreasonably withholding or delaying, as appropriate, its approval of the draft Remediation Action Plan; and

(d) would not have occurred had:

(i) the Authority given its approval, or given its approval in a timely manner, to the draft Remediation Action Plan; and

(ii) 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:

(a) provide the Authority with a full, unedited and unredacted copy of the test report;

(b) implement interim mitigation measures to vulnerabilities in the Information System known to be exploitable where a security patch is not immediately available;

(c) as far as practicable, remove or disable any extraneous interfaces, services or capabilities not needed for the provision of the Services within the timescales set out in the test report or such other timescales as may be agreed with the Authority.

**Significant vulnerabilities**

12.21 Where:

(a) a Security Test report identifies more than 10 vulnerabilities classified as either critical or high; or

(b) the Authority rejected a revised draft Remediation Action Plan,

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

(c) appoint an independent and appropriately qualified and experienced security architect and adviser to perform a root cause analysis of the identified vulnerabilities; or

(d) 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:

(a) identify and authenticate all persons who access the Supplier Information Management System and Sites before they do so;

(b) require multi-factor authentication for all user accounts that have access to Authority Data or that are Privileged Users;

(c) allow access only to those parts of the Supplier Information Management System and Sites that those persons require;

(d) maintain records detailing each person's access to the Supplier Information Management System and Sites, and make those records available to the Authority on request.

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:

(a) are allocated to a single, individual user;

(b) are accessible only from dedicated End-user Devices;

(c) are configured so that those accounts can only be used for system administration tasks;

(d) require passwords with high complexity that are changed regularly;

(e) 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

(f) are:

(i) restricted to a single role or small number of roles;

(ii) time limited; and

(iii) 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:

(a) 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

(b) 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 Authority Data and the Code to:

(a) identify and prevent potential Breaches of Security;

(b) respond effectively and in a timely manner to Breaches of Security that do occur;

(c) identify and implement changes to the Supplier Information Management System to prevent future Breaches of Security; and

(d) 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:

(a) event logs and audit records of access to the Supplier Information Management system; and

(b) regular reports and alerts to identify:

(i) changing access trends;

(ii) unusual usage patterns; or

(iii) the access of greater than usual volumes of Authority Data;

(c) the detection and prevention of any attack on the Supplier Information Management System or the Development Environment using common cyber-attack techniques;

(d) any other matters required by the Security Management Plan.

**Event logs**

14.3 The Supplier must ensure that, unless the Authority otherwise agrees, any event logs do not log:

(a) personal data, other than identifiers relating to users; or

(b) sensitive data, such as credentials or security keys.

**Provision of information to Authority**

14.4 The Supplier must provide the Authority on request with:

(a) full details of the Protective Monitoring System it has implemented; and

(b) copies of monitoring logs and reports prepared as part of the Protective Monitoring System.

**Changes to Protective Monitoring System**

14.5 The Authority may at any time require the Supplier to update the Protective Monitoring System to:

(a) respond to a specific threat identified by the Authority;

(b) implement additional audit and monitoring requirements; and

(c) stream any specified event logs to the Authority's security information and event management system.

## 15 Audit rights

**Right of audit**

15.1 The Authority may undertake an audit of the Supplier or any Sub-contractor to:

(a) verify the Supplier's or Sub-contractor's (as applicable) compliance with the requirements of this Schedule 5 (*Security Management*) and the Data Protection Laws as they apply to Authority Data;

(b) inspect the Supplier Information Management System (or any part of it);

(c) review the integrity, confidentiality and security of the Authority Data; and/or

(d) review the integrity and security of the Code.

15.2 Any audit undertaken under Paragraph 15.1:

(a) may only take place during the Term and for a period of 18 months afterwards; and

(b) is in addition to any other rights of audit the Authority has under this Contract.

15.3 The Authority may not undertake more than one audit under Paragraph 15.1 in each calendar year unless the Authority has reasonable grounds for believing:

(a) the Supplier or any Sub-contractor has not complied with its obligations under this Contract or the Data Protection Laws as they apply to the Authority Data;

(b) there has been or is likely to be a Breach of Security affecting the Authority Data or the Code; or

(c) where vulnerabilities, or potential vulnerabilities, in the Code have been identified by:

(i) an IT Health Check; or

(ii) a Breach of Security.

**Conduct of audits**

15.4 The Authority must use reasonable endeavours to provide 15 Working Days' notice of an audit.

15.5 The Authority must when conducting an audit:

(a) comply with all relevant policies and guidelines of the Supplier or Sub-contractor (as applicable) concerning access to the Suppler Information Management System the Authority considers reasonable having regard to the purpose of the audit; and

(b) 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 Authority with all co-operation and assistance the Authority may reasonably require, including:

(a) all information requested by the Authority within the scope of the audit;

(b) access to the Supplier Information Management System; and

(c) access to the Supplier Staff.

**Response to audit findings**

15.7 Where an audit finds that:

(a) the Supplier or a Sub-contractor has not complied with this Contract or the Data Protection Laws as they apply to the Authority Data; or

(b) there has been or is likely to be a Security Breach affecting the Authority Data

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

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

## 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:

(a) minimise the extent of actual or potential harm caused by such Breach of Security;

(b) remedy such Breach of Security to the extent possible;

(c) apply a tested mitigation against any such Breach of Security; and

(d) 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 Authority, provide to the Authority:

(a) full details of the Breach of Security; and

(b) if required by the Authority:

(i) a root cause analysis; and

(ii) a draft plan addressing the Breach of Security

(a **Breach Action Plan**).

16.4 The draft Breach Action Plan must set out:

(a) in respect of each issue identified in the root cause analysis:

(i) how the issue will be remedied;

(ii) the date by which the issue will be remedied; and

(iii) the tests that the Supplier proposes to perform to confirm that the issue has been remedied or the finding addressed;

(b) the assistance the Supplier will provide to the Authority to resolve any impacts on the Authority, the Authority Data and the Code;

(c) 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;

(d) 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 Authority with such technical and other information relating to the draft Breach Action Plan as the Authority requests.

16.6 The Authority may:

(a) 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:

(i) the Supplier shall within ten Working Days of the date on which the Authority rejected the draft Breach Action Plan, or such other period as the Authority requires, submit a revised draft Breach Action Plan that takes into account the Authority's reasons; and

(ii) Paragraph 16.5 and 16.6 shall apply to the revised draft Breach Action Plan;

(b) 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:

(a) establish infrastructure, services and systems referred to in the Breach Action Plan;

(b) communicate and engage with affected individuals in accordance with the Breach Action Plan;

(c) communicate and engage with the Authority and stakeholders identified by the Authority in accordance with the Breach Plan and as otherwise required by the Authority; and

(d) engage and deploy such additional resources as may be required to perform its responsibilities under the Breach Plan and this Contract in respect of the Personal Data Breach without any impact on the provision of the Services;

(e) continue to implement the Breach Action Plan until the Authority indicates that the Breach of Security and the impacts on the Authority, the Authority Data, the Code and the affected individuals have been resolved to the Authority'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 this 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:

(a) make that report within the time limits:

(i) specified by the relevant regulator; or

(ii) otherwise required by Law;

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

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

(a) provide such information and other input as the Authority requires within the timescales specified by the Authority;

(b) ensure so far as practicable the report it sends to the relevant regulator is consistent with the report provided by the Authority.

## 17 Exit management

17.1 In addition to any obligations on the Supplier under Schedule 25 (*Exit Management*) the Supplier must:

(a) agree with the Authority and, where required by the Supplier, the Replacement Supplier; and

(b) document as part of the Exit Plan,

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

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

(a) the data formats of the Authority Data;

(b) the roles and responsibilities of the Supplier, the Authority and (where applicable) the Replacement Supplier;

(c) the methods to be used to securely transfer the data;

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

(e) how data migration will be managed to ensure continuity of Services and the integrity, confidentiality and accessibility of the Authority 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 Authority Data

18.1 The Supplier must create and maintain a register of:

(a) all Authority Data the Supplier, or any Sub-contractor, receives from or creates for the Authority; and

(b) 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 Authority Data is stored,

(**Authority Data Register**).

18.2 The Supplier must:

(a) review and update the Authority Data Register:

(i) within ten Working Days of the Supplier or any Sub-contractor changes to those parts of the Supplier Information Management System on which the Authority Data is stored;

(ii) within ten Working Days of a significant change in the volume, nature or overall sensitivity of the Authority Data stored on the Supplier Information Management System;

(iii) at least once every 12 months; and

(b) provide the Authority with a copy of the Authority Data Register:

(i) whenever it updates the Authority Data Register; and

(ii) otherwise when the Authority requests.

18.3 Subject to Paragraph 18.4, the Supplier must, and must ensure that all Sub-contractors, securely erase any or all Authority Data held by the Supplier or Sub-contractor, including any or all Code:

(a) when requested to do so by the Authority; and

(b) using a deletion method agreed with the Authority that ensures that even a determined expert using specialist techniques can recover only a small fraction of the data deleted.

18.4 Paragraph **Error! Reference source not found.** does not apply to Authority Data:

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

(b) to which the Supplier has rights to Handle independently from this Contract; or

(c) 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 Authority with copies of any or all Authority Data held by the Supplier or Sub-contractor, including any or all Code:

(a) when requested to do so by the Authority; and

(b) using the method specified by the Authority.

# Appendix 2 Security Requirements for Development

## 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:

(a) no Malicious Software is introduced into the Developed System or the Supplier Information Management System.

(b) the Developed System can continue to function in accordance with the Specification:

(i) in unforeseen circumstances; and

(ii) 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:

(a) comply with the Secure Development Guidance as if its requirements were terms of this Contract; and

(b) 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:

(a) ensure that all Supplier Staff engaged in Development Activity are:

(i) trained and experienced in secure by design code development;

(ii) provided with regular training in secure software development and deployment;

(b) ensure that all Code:

(i) is subject to a clear, well -organised, logical and documented architecture;

(ii) follows OWASP Secure Coding Practice

(iii) follows recognised secure coding standard, where one is available;

(iv) employs consistent naming conventions;

(v) is coded in a consistent manner and style;

(vi) is clearly and adequately documented to set out the function of each section of code;

(vii) is subject to appropriate levels of review through automated and non-automated methods both as part of:

(A) any original coding; and

(B) at any time the Code is changed;

(c) ensure that all Development Environments:

(i) protect access credentials and secret keys;

(ii) is logically separate from all other environments, including production systems, operated by the Supplier or Sub-contractor;

(iii) requires multi-factor authentication to access;

(iv) have onward technical controls to protect the Developed System or the Supplier Information Management System in the event a Development Environment is compromised; and

(v) 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:

(a) the NCSC's guidance on "Security Design Principles for Digital Services";

(b) where the Developed System will Handle bulk data, the NCSC's guidance on "Bulk Data Principles"; and

(c) 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 this Contract, the Supplier must ensure that the Developed System encrypts Authority Data:

(a) when the Authority Data is stored at any time when no operation is being performed on it; and

(b) when the Authority 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 the Security Requirements.

## 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:

(a) regularly; or

(b) as required by the Authority

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 Authority:

(a) the modules or elements of the Code subject to the Code Review;

(b) the development state at which the Code Review will take place;

(c) any specific security vulnerabilities the Code Review will assess; and

(d) 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:

(a) must undertake Code Reviews in accordance with the Code Review Plan; and

(b) 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 or each Code Review, the Supplier must provide the Authority 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:

(a) remedy these at its own cost and expense;

(b) ensure, so far as reasonably practicable, that the identified security vulnerabilities are not present in any other modules or code elements; and

(c) modify its approach to undertaking the Development Activities to ensure, so far as is practicable, the identified security vulnerabilities will not re-occur; and

(d) provide the Authority 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 Authority Data where the licence terms of that software purport to grant the licensor rights to Handle the Authority 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:

(a) 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;

(b) perform adequate due diligence to determine whether there are any recognised security vulnerabilities with that Third-party Software Module;

(c) continue to monitor any such Third-party Software Module so as to ensure it promptly becomes aware of any newly -discovered security vulnerabilities;

(d) 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(b), 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:

(a) full details of the developer of the module;

(b) the due diligence the Supplier undertook on the Third-party Software Module before deciding to use it;

(c) any recognised security vulnerabilities in the Third-party Software Module; and

(d) how the Supplier will minimise the effect of any such security vulnerability on the Developed System.

7.5 The Supplier must:

(a) review and update the Modules Register:

(i) within 10 Working Days of becoming aware of a security vulnerability in any Third-party Software Module; and

(ii) at least once every six months;

(b) provide the Authority with a copy of the Modules Register:

(i) whenever it updates the Modules Register; and

(ii) otherwise when the Authority requests.

# Appendix 3 Security Working Group

## 1 Role of the Security Working Group

1.1 The Security Working Group shall be responsible for the [insert remit of Security Working Group].

1.2 The Security Working Group:

(a) monitors and provides recommendations to the Supplier on the assurance of the Supplier Information Management System;

(b) provides a forum for the sharing of information concerning security risks and threats and determining the appropriate mitigations;

(c) [insert remainder of terms of reference for Security Working Group].

## 2 Meetings of the Security Working Group

Paragraphs 3.4 to 3.7 of Schedule 21 (Governance) shall apply to the Security Working Group as if it were a Board established under that Schedule.

## 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 Woking Group:

(a) [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

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

| | SIMS Sub-contractors | Higher-risk Sub-contractors | Medium-risk Sub-contractors | Sub-contractors |
|---|---|---|---|---|
| Security Requirements that do not apply | | | | |
| Development Requirements that do not apply | | | | |

# Appendix 5 Security Management Plan Template

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

# Appendix 6 Secure by Design Principles Evaluation Table

## 1 Completion of Principles Evaluation Table

1.1 As part of the Security Management Plan, the Supplier must complete the table in this Appendix 6 (*Secure by Design Principles Evaluation Table*), unless that requirement is waived by the Authority.

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**<br>Create responsibility for cyber security risk<br>Assign a designated risk owner to be accountable for managing cyber security risks for the service within the contract. This must be a senior stakeholder with the experience, knowledge and authority to lead on security activities. | 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 infrastructure during their delivery. | |
| | The Supplier provides adequate and appropriately qualified resources to support the Authority with following the government Secure by Design approach as part of service delivery. | |

| Secure by Design Principle | Requirements | How the Supplier will meet the requirement |
|---|---|---|
| | These resources must be reviewed at the beginning of each of the delivery phases during the delivery lifecycle of the service as agreed with the Authority. | |
| **Principle 2**<br>Source secure technology products<br>Where third-party products are used, perform security due diligence by continually assessing platforms, software and code for security vulnerabilities. Mitigate risks and share findings with suppliers to help them improve product security. | The Supplier carries out proportionate (risk-driven) security reviews of third-party products before they are considered as a component of the digital service. The type and details of the review should be based on the significance associated with the product and are subject to agreement with the Authority. | |
| | The Supplier takes reasonable steps to reduce potential cyber security risks associated with using a third-party product as part of the service to a level that meets the Authority's security risk appetite for the service. Where the risk cannot be mitigated to such level, the Authority should be informed and asked to accept the risk associated with using the product. | |
| | The Supplier takes reasonable steps to assess third-party products used as a component of the digital service against legal and regulatory obligations and industry security standards specified by the Authority. Where the product | |

| Secure by Design Principle | Requirements | How the Supplier will meet the requirement |
|---|---|---|
| | doesn't meet the required obligations, the Supplier must discuss with the Authority the residual risks associated with using the product. | |
| **Principle 3**<br>Adopt a risk-driven approach<br>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 Authority, the Supplier should share the risk appetite across the supplier's delivery team from the outset. | |
| | The Supplier supports the Authority with identifying the cyber threats and attack paths as part of ongoing threat modelling during digital service delivery. | |
| | The Supplier supports the Authority with assessing cyber security risks and providing risk analysis details to help risk owners make informed risk decisions.<br>During the assessment, risks to the digital service are identified, analysed, prioritised, and appropriate mitigation is proposed taking into account the risk appetite during the lifecycle of the service. | |
| | 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 | |

| Secure by Design Principle | Requirements | How the Supplier will meet the requirement |
|---|---|---|
| | appetite and cyber security risk management approach. | |
| | The Supplier factors in the legal and regulatory requirements provided by the Authority in the risk management process and service design and build. | |
| **Principle 4**<br>Design usable security controls<br>Perform regular user research and implement findings into service design to make sure security processes are fit for purpose and easy to understand. | The Supplier ensures that security requirements that are defined and documented as part of user research activities (for example user stories and user journeys) are fed into the design of the digital service. | |
| | 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. | |
| **Principle 5**<br>Build in detect and respond security<br>Design for the inevitability of security vulnerabilities and incidents. Integrate appropriate security logging, monitoring, alerting and response capabilities. These must be continually tested and iterated. | 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. | |
| | The Supplier responsible for building the digital service | |

| Secure by Design Principle | Requirements | How the Supplier will meet the requirement |
|---|---|---|
| | 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**<br>Design flexible architectures<br>Implement digital services and update legacy components to allow for easier integration of new security controls in response to changes in business requirements, cyber threats and vulnerabilities. | As agreed with the Authority, the Supplier responsible for building the digital service uses flexible architectures and components that allow integration of new security measures in response to changes in business requirements, cyber threats and vulnerabilities. | |
| | The Supplier responsible for building the digital service tests security controls and verifying they are fit for purpose before deployment. | |
| **Principle 7**<br>Minimise the attack surface<br>Use only the capabilities, software, data and hardware components necessary for a | The Supplier responsible for building the digital service implements risk-driven security controls which meet the risk appetite and appropriate baseline as agreed with the Authority. | |

| Secure by Design Principle | Requirements | How the Supplier will meet the requirement |
|---|---|---|
| service to mitigate cyber security risks while achieving its intended use. | The Supplier responsible for building the digital service follows secure coding practices and, with consultation with the Authority's delivery team, identifies and mitigates vulnerabilities proactively reducing the number of vulnerabilities that potential attackers can exploit. | |
| | The Supplier retires service components (including data) securely when they are no longer needed, or at the end of their lifecycle. | |
| **Principle 8**<br>Defend in depth<br>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. | |