Schedule 16 (Security)

Contents

1 Authority Options

1.1 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:

Locations (see paragraph 1 of the Security Requirements)		
The Supplier and Sub-contractors may store, access or Process Government Data in:	the United Kingdom only	☐
	the United Kingdom and European Economic Area only	X
	anywhere in the world not prohibited by the Buyer	☐
Support Locations (see paragraph 1 of the Security Requirements)		
The Supplier and Subcontractors may operate Support Locations in:	the United Kingdom only	☐
	the United Kingdom and European Economic Area only	X
	anywhere in the world not prohibited by the Buyer	☐
Development Activity (see Appendix 1 (*Security Requirements for Development*))		
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	☐
	the United Kingdom and European Economic Area only	☐
	anywhere in the world not prohibited by the Buyer	☐

2 Definitions

Anti-virus Software	means software that: (a) protects the Supplier Information Management System from the possible introduction of Malicious Software; (b) scans for and identifies possible Malicious Software in the Supplier Information Management System;

	(c) if Malicious Software is detected in the Supplier Information Management System, so far as possible: (i) prevents the harmful effects of the Malicious Software; and (ii) removes the Malicious Software from the Supplier Information Management System.
Assets	means all assets and rights used by the Supplier to provide the Services in accordance with this Contract but excluding the Authority Assets.
Authority Data	means any: (a) data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media; (b) Personal Data for which the Authority is a, or the, Data Controller; or (c) any meta-data relating to categories of data referred to in paragraphs (a) or (b); that is: (d) supplied to the Supplier by or on behalf of the Authority; or (e) that the Supplier generates, processes, stores or transmits under this Contract; and for the avoidance of doubt includes the Code and any meta-data relating to the Code.
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 16 of the Security Requirements.
Authority Equipment	means any hardware, computer or telecoms devices, and equipment that forms part of the Authority System.
Authority Premises	means premises owned, controlled or occupied by the Authority and/or any Central Government Body which are made available for use by the Supplier or its Sub-contractors for provision of the Services (or any part of the Service).
Authority System	means the Authority's information and communications technology system, including any software or Authority Equipment, owned by the Authority or leased or licenced to it by a third-party, that: (a) is used by the Authority or the Supplier in connection with this contract; (b) interfaces with the Supplier System; and/or

	(c) is necessary for the Authority to receive the Services.
Breach Action Plan	means a plan prepared under paragraph 14.3 of the Security Requirements addressing any Breach of Security.
Breach of Security	means the occurrence of: (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; (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 (c) any part of the Supplier Information Management System ceasing to be compliant with the Certification Requirements; (d) the installation of Malicious Software in the: (i) Supplier Information Management System; (ii) Development Environment; or (iii) Developed System; (e) any loss of operational efficiency or failure to operate to specification as the result of the installation or operation of Malicious Software in the: (i) Supplier Information Management System; (ii) Development Environment; or (iii) Developed System; and (f) includes any attempt to undertake the activities listed in sub-paragraph (a) where the Supplier has reasonable grounds to suspect that attempt: (i) was part of a wider effort to access information and communications technology operated by or on behalf of Central Government Bodies; or (ii) was undertaken, or directed by, a state other than the United Kingdom.
Certification Requirements	means the requirements set out in paragraph 12.3.

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: (a) has been certified by the National Cyber Security Centre; (g) holds "Green Light" status; and (h) is authorised to provide the IT Health Check services required by paragraph 10 of the Security Requirements.
Code	means, in respect of the Developed System: (a) the source code; (i) the object code; (j) third-party components, including third-party coding frameworks and libraries; and (k) all supporting documentation.
Code Review	means a periodic review of the Code by manual or automated means to: (a) identify and fix any bugs; and (b) ensure the Code complies with (i) the requirements of this Schedule [*****] (*Security Management*); and (ii) the Secure Development Guidance.
Code Review Plan	means the document agreed with the Authority under paragraph 5.2 of the Security Requirements 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 15.1 of the Security Requirements.

Developed System	means any software or system that the Supplier will develop under this Contract either: (a) as part of the Services; or (c) to create or modify Software to: (i) provide the Services; or (ii) Process Authority Data.
Development Activity	means any activity relating to the development, deployment maintenance and upgrading of the Developed System, including: (a) coding; (b) testing; (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.
EEA	means the European Economic Area.
End-user Device	means any personal computers, laptops, tablets, terminals, smartphones or other portable electronic device 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.
Higher Risk Sub-contractor	means a Sub-contractor that Processes Authority Data, where that data includes either: (a) 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(b); or (b) any part of that Personal Data includes any of the following: (i) financial information (including any tax and/or welfare information) relating to any person; (ii) any information relating to actual or alleged criminal offences (including criminal records); (iii) any information relating to children and/or vulnerable persons;

	(iv) any information relating to social care; (v) any information relating to a person's current or past employment; or (vi) Special Category Personal Data; or (c) the Authority in its discretion, designates a Sub-contractor as a Higher Risk Sub-Contractor: (i) in any procurement document related to this Contract; or (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 6.0, May 2018 (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/714002/HMG_Baseline_Personnel_Security_Standard_-_May_2018.pdf), 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 18.
ISO Certification	means: (a) ISO/IEC27001:2013, where the certification was obtained before November 2022, but only until November 2025; and (d) 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	means any Sub-contractor: (a) which, in the opinion of the Authority, performs (or would perform if appointed) a critical role in the provision of all or any part of the Services; and/or (b) with a Sub-contract with a contract value which at the time of appointment exceeds (or would exceed if appointed) 10% of the aggregate Charges forecast to be payable under this Contract (as set out in the Financial Model).
Key Sub-contractor Default	has the meaning set out in paragraph 10.4.
Malicious Software	any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether

	the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Medium Risk Sub-contractor	means a Sub-contractor that Processes Authority Data, [where that data (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(b); and (c) does not include Special Category Personal Data.
Modules Register	means the register of Third-party Software Modules required by paragraph 7.2 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-security/implementing-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.
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/migrated_content.
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.
Process	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.
Prohibited Activity	means the storage, access or Processing of Authority Data prohibited by a Prohibition Notice.
Prohibition Notice	means a notice issued under paragraph 1.10 of the Security Requirements.
Protective Monitoring System	means the system implemented by the Supplier and its Sub-contractors under paragraph 12.1 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 17.1.
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: (a) the Sites, Support Locations and Third-party Tools that the Supplier will use to Process Authority Data or provide the Services; (b) the nature of the activity performed at the Site or Support Location or by the Third-Party Tool in respect of the Authority Data; (c) in respect of each entity providing a Site, Support Location or Third-Party Tool, its: (i) full legal name; (ii) trading name (if any) (iii) country of registration; (iv) registration number (if applicable); and (v) registered address.
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: (a) the details of any approval of the change provided by the Authority, including any conditions or limitations on that approval; and (d) the date: (i) the date by which the change it to be implemented; and (ii) the date on which the change was implemented.

Residual Risk Statement	means a notice issued by the Authority that (a) sets out the information risks associated with using the Supplier Information Management System; and (e) confirms that the Authority: (i) is satisfied that the identified risks have been adequately and appropriately addressed; and (ii) that the residual risks are understood and accepted by the Authority.
Relevant Activities	means those activities specified in paragraph 1.1 of the Security Requirements.
Relevant Certifications	means: (a) in the case of the Supplier, any SIMS Sub-contractor and any Sub-contractor that Processes Authority Data: (i) an ISO Certification by a UKAS-approved certification body in respect of the Supplier Information Management System, or the Supplier Information Management System is included within the scope of a wider certification of compliance with an ISO Certification; and (ii) Cyber Essentials Plus; and (f) for all other Sub-contractors means Cyber Essentials Plus.
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 10.20 to 10.24, addressing the vulnerabilities and findings in a IT Health Check report
Risk Management Approval Statement	the statement issued by the Authority under paragraph 15.2 following the Authority-led Assurance of the Supplier Information Management System.
Secure Development Guidance	means the Supplier's secure coding policy required under its ISO27001 Relevant Certification.
Security Management Plan	means the document prepared in accordance with the requirements of paragraph 13 and in the format, and containing the information, specified in Appendix 5.

Security Requirements	mean the security requirements in Appendix 1 to this Schedule [x] (*Security Management*)
Security Requirements for Development	means the security requirements in Appendix 1 to this Schedule [x] (*Security Management*)
Security Test	means: (a) an Authority Security Test; (g) an IT Health Check; or (h) 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.
Sites	means any premises (including the Authority Premises, the Supplier's premises or third-party premises): (a) from, to or at which: (i) the Services are (or are to be) provided; or (ii) the Supplier or any Sub-contractor manages, organises or otherwise directs the provision or the use of the Services; or (i) where: (i) any part of the Supplier System is situated; or (ii) any physical interface with the Authority System takes place.
SMP Sub-contractor	means a Sub-contractor with significant market power, such that: (a) they will not contract other than on their own contractual terms; and (j) either: (i) there are no other substitutable suppliers of the particular services other than SMP Sub-contractors; or (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 13.1 setting out the nature and level of risk that the Supplier accepts from the operation of the Supplier Information Management System.
Sub-contractor	includes, for the purposes of this Schedule [x] (*Security Management*), any individual or entity that: (a) forms part of the supply chain of the Supplier; and (k) 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.
Sub-contractor Personnel	means: (a) any individual engaged, directly or indirectly, or employed, by any Sub-contractor; and (l) engaged in or likely to be engaged in: (i) the performance or management of the Services; (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: (a) the Software; (m) the Supplier Equipment; (n) configuration and management utilities; (o) calibration and testing tools; (p) and related cabling; but does not include the Authority System.
Supplier Information Management System	means (a) the Supplier System; (q) the Sites; (r) any part of the Authority System the Supplier or any Sub-contractor will use to Process Authority Data, or provide the Services; and (s) the associated information management system, including all relevant:

	(i) organisational structure diagrams, (ii) controls, (iii) policies, (iv) practices, (v) procedures, (vi) processes; and (vii) resources.
Supplier Personnel	means any individual engaged, directly or indirectly, or employed by the Supplier or any Sub-contractor, in the management or performance of the Supplier's obligations under this Contract.
Supplier System	means the information and communications technology system used by the Supplier or any Sub-contractor in implementing and performing the Services including any software, hardware, computer and telecoms devices, equipment, configuration and management utilities, calibration and testing tools and related cabling (but excluding the Authority System).
Support Location	means a place or facility where or from which individuals may access or Process 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 4 of the Security Requirements.
Third-party Software Module	means any module, library or framework that: (a) is not produced by the Supplier or a Sub-contractor as part of the Development Activity; and (t) either: (i) forms, or will form, part of the Code; or (ii) is, or will be, accessed by the Developed System during its operation.
Third-party Tool	means any activity conducted other than by the Supplier during 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.
Wider Information Management System	means (a) any: (i) information assets,

(ii) IT systems,

(iii) IT services; or

(iv) Sites,

that the Supplier or any Sub-contractor will use to:

(i) Process, or manage or support the Processing of, Authority Data; or

(ii) provide, or manage or support the provision of, the Services; or

(u) any IT systems controlled or operated by the Supplier or any Sub-contractor that interface with such information assets, IT systems, IT services or Sites;

(v) together with the associated information management system, including all relevant:

(i) organisational structure diagrams,

(ii) controls,

(iii) policies,

(iv) practices,

(v) procedures,

(vi) processes; and

(vii) resources.

3 Introduction

3.1 This Schedule [x] (*Security Management*) sets out:

(a) the Authority's decision on where the Supplier may:

(i) store, access or process Authority Data;

(ii) undertake the Development Activity;

(iii) host the Development Environment; and

(iv) locate Support Locations,

(in paragraph 1)

(b) the principles of security that apply to this Contract (in paragraph 4);

(c) the requirement to obtain a Risk Management Approval Statement (in paragraphs 6 and 15;

(d) the annual confirmation of compliance to be provided by the Supplier (in paragraph 7);

(e) the governance arrangements for security matters, where these are not otherwise specified in Schedule [x] (*Governance*) (in paragraph 8);

(f) access to personnel (in paragraph 9);

(g) obligations in relation to Sub-contractors (in paragraph 10);

(h) the responsibility of the Supplier to determine the Supplier Information Management System (in paragraph 11);

(i) the Certification Requirements (in paragraph 12);

(j) the development, monitoring and updating of the Security Management Plan by the Supplier (in paragraphs 13, 14 and 15);

(k) the granting by the Authority of approval for the Supplier to commence:

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

(ii) Processing Authority Data (in paragraph 6);

(l) the management of changes to the Supplier Information Management System (in paragraph 16); and

(m) the Authority's additional remedies for breach of this Schedule [x] (*Security Management*), including:

(i) the requirement for Remediation Action Plans (in paragraph 17);

(ii) the appointment of Independent Security Advisers (in paragraph 18); and

(iii) the withholding of Charges by the Authority (in paragraph 19).

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.

(f) 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.

(g) Notwithstanding any approvals or agreements provided by the Authority under this Schedule [x] (*Security Management*), the Supplier remains responsible for:

(i) 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

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

5 Security requirements

5.1 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 (Authority Options) is selected, comply with the Security Requirements for Development in Appendix 1; and

(c) ensure that Sub-contractors comply with:

(i) all Security Requirements in Appendix 1; and

(ii) where the relevant option in paragraph 1 (*Authority Options*) is selected, all Security Requirements for Development in Appendix 1,

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

(A) paragraph 5.2 applies; or

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

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

(a) use best endeavours to ensure that the SMP Sub-contractor complies with the Security Requirements;

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

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

6 Authority to proceed

6.1 Notwithstanding anything in this Contract, the Supplier may not:

(a) commence the provision of any Operational Services; or

(b) Process any Authority Data using the Supplier Information Management System,

unless:

(i) the Supplier has, and ensured that Sub-contractors have, obtained the Relevant Certifications under paragraph 12;

(ii) the Supplier has completed an IT Health Check in accordance with paragraph 10 of the Security Requirements; and

(iii) the Authority has issued a Risk Management Approval Statement under paragraph 15.

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 [x] (Security Management); and

(ii) all Sub-contractors have complied with the requirements of this Schedule [x] (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 [x] (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

8.1 This paragraph 8 applies where a Security Working Group, or Board (as that term is defined in Schedule [x] (*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) once every Contract Year following the review of the Security Management Plan by the Supplier under paragraph 14 and before the Authority has completed its review of the updated Security Management Plan under paragraph 15; 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 the Authority agrees otherwise; and

(b) do not limit or modify the Supplier's responsibilities under this Schedule [x] (*Security Management*)

8.8 Appendix 3 applies to the Security Working Group.

9 Personnel

9.1 The Supplier must ensure that it 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 [x] (Security Management).

9.2 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:

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

(ii) the Authority shall provide access to its personnel responsible for information assurance.

10 Sub-contractors

SIMS Sub-contractor

10.1 Notwithstanding anything else in this Contract, but subject to paragraph 5.2, a SIMS Sub-contractor shall be treated for all purposes as a Key Sub-contractor.

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

Sub-contractors

10.3 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 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

10.4 Where the Supplier becomes aware of an actual or suspected failure by a Key Sub-contractor to comply with any obligation in this Schedule with which the Supplier is, by virtue of paragraph 5.1, 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 2 Working days of becoming aware of the Key Sub-contractor Default notify the Authority setting out the actual or anticipated effect of the Key Sub-contractor Default; and

(b) unless the Authority waives the requirement, comply with the Remediation Action Plan process in paragraph 17.

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 the 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 determination 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:

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

(ii) requires approval by the Authority under paragraph 16; and

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

12 Certification Requirements

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

(a) it; and

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

(i) an ISO Certification by a UKAS-approved certification body in respect of the Supplier Information Management System, or the Supplier Information Management System is included within the scope of a wider certification of compliance with an ISO Certification; and

(ii) Cyber Essentials Plus; and

(d) for all other Sub-contractors, Cyber Essentials Plus.

12.2 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.

12.3 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) 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**).

12.4 The Supplier must notify the Authority promptly, and in any event within 3 Working Days, after becoming aware that, in respect of it or any Sub-contractor:

(a) a Relevant Certification has been revoked or cancelled by the body that awarded it;

(b) a Relevant Certification expired and has not been renewed by the Supplier;

(c) a Relevant Certification no longer applies 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**)

12.5 Where the Supplier has notified the Authority of a Certification Default under paragraph 12.4:

(a) the Supplier must, within 10 Working Days of the date in which the Supplier provided notice under paragraph 12.4 (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 5 Working Days of the date of the rejection submit a revised Certification Rectification Plan and paragraph 12.5(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 Buyer accepts the Certification Rectification Plan, the Supplier must start work immediately on the plan.

13 Security Management Plan

Purpose of Security Management Plan

13.1 The Authority may, at any time, provide the Supplier with a Statement of Risk Appetite.

13.2 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 [x] (*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).

13.3 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 [x] (*Security Management*) and the Statement of 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 Risk Appetite (where one has been provided).

Preparation of Security Management Plan

13.4 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 to review and approve the Security Management Plan before the first Operational Service Commencement Date.

13.5 If paragraph 13.4(b) applies, and any delay resulting from the Authority's review and approval of the Security Management Plan 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

13.6 The Security Management Plan must use the template in Appendix 5 and 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, the controls the Supplier will implement in respect of the Services and all processes associated with the delivery of the Services, including in respect of:

(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;

(e) the Required Changes Register;

(f) 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 (*Authority Options*) is selected, the Security Requirements for Development;

(g) the diagram documenting the Supplier Information Management System, the Wider Information Management System and the boundary between them (created under paragraph 11);

(h) an assessment of the Supplier Information Management System against the requirements of this Schedule [x] (*Security Management*), including the Security Requirements and, where the relevant option in paragraph 1 (*Authority Options*) is selected, the Security Requirements for Development;

(i) 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

(j) 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 Processed by the Sub-contractor;

(vii) the Processing 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 [x] (*Security Management*);

(k) the Register of Sites, Support Locations and Third Party Tools;

(l) the Modules Register;

(m) the Support Register; and

(n) details of the protective monitoring that the Supplier will undertake in accordance with paragraph 12 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.

14 Monitoring and updating Security Management Plan

Updating Security Management Plan

14.1 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

14.2 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 Processes Authority Data;

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

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

must:

(i) within 2 Working Days notify the Authority; and

(ii) within 10 Working Days, or such other timescale as may be agreed with the Authority:

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

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

14.3 paragraph 14.2 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.

14.4 Any proposed change under paragraph 14.2(a), 14.2(b) or 14.2(f) is a Contract Change to which the Change Control Procedure applies.

15 Review and approval of Security Management Plan

15.1 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.

15.2 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 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.

16 Changes to the Supplier Information Management System

16.1 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 Processes Authority Data.

16.2 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 the Supplier proposes to implement those changes.

16.3 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.

16.4 If the Authority does not provide a decision within the period specified in paragraph 16.3(b), the proposal shall be deemed to have been accepted.

Implementation of changes

16.5 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.

16.6 If the Supplier does not implement a necessary change to the Supplier Information Management System to address a security related risk or vulnerability:

(a) that failure is a material Default; and

(b) the Supplier shall:

(i) immediately cease using the Supplier Information Management System to Process 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).

17 Remediation Action Plan (RAP)

Preparation of Remediation Action Plan

17.1 This paragraph 17 applies when:

(a) 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**).

17.2 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**).

17.3 The 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

17.4 The Supplier must

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

(b) have regarded 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 a Remediation Action Plan

17.5 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 been fully and correctly implemented.

17.6 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.

18 Independent Security Adviser

18.1 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 15.2(b)); or

(c) a Security Test (see paragraph 10 of the Security Requirements) report identifies more than 10 vulnerabilities classified as either critical or high.

18.2 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 person(s) 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.

18.3 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.

18.4 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.

18.5 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).

18.6 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.

18.7 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 18,

this is a material Default that is capable of remedy.

19 Withholding of Charges

19.1 The Authority may withhold some or all of the Charges in accordance with the provisions of this paragraph 19 where:

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

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

(i) a Notifiable Default;

(ii) an Intervention Cause; or

(iii) a Step-in Trigger Event.

19.2 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.

19.3 Before withholding any Charges under paragraph 19.1 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.

19.4 Where the Supplier does not remedy the Default by the date specified in the notice given under paragraph 19.3(a), the Authority may retain the withheld amount.

19.5 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 [x] (*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

19.6 The Authority's right to withhold or retain any amount under this paragraph 19 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.

20 Access to Authority System

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.

Signature page

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;

(i) the Supplier Information Management System; or

(ii) the Wider Information Management System;

(c) store, access or process 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 the United Kingdom.

1.3 Where the Authority has permitted the Supplier and its Sub-contractors to perform the Relevant Activities outside the United Kingdom or European Economic Area, 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 [x] (*Security Management*);

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

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

(i) the entity;

(i) the arrangements with the entity; and

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

(c) the Authority has not given the Supplier a Prohibition Notice under paragraph 1.10.

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 process 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 process 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 the United Kingdom.

1.7 Where the Authority has permitted the Supplier and its Sub-contractors to operate Support Locations outside the United Kingdom or European Economic Area, 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 [x] (*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

(iv) the Authority has not given the Supplier a Prohibition Notice under paragraph 1.10.

Third-party Tools

1.8 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.

1.9 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

1.10 The Authority may by notice in writing at any time give notice to the Supplier that it and its Sub-contractors must not undertake or permit to be undertaken some or all of the Relevant Activities or operate Support Locations (**Prohibited Activity**).

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

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

(c) in or using any particular facility or group of facilities, whether operated by the Supplier, a Sub-contractor or a third-party entity (**Prohibition Notice**).

1.11 Where the Supplier or Sub-contractor, on the date of the Prohibition Notice undertakes any Relevant Activities or operates any Support Locations affected by the notice, the Supplier must, and must procure that Sub-contractors, cease to undertake that Prohibited Activity within 40 Working Days of the date of the Prohibition Notice.

2 Vetting, Training and Staff Access

Vetting before performing or managing Services

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

(a) Development Activity;

(b) any activity that provides access to the Development Environment; or

(c) any activity relating to the performance and management of the Services unless:

(i) that individual has passed the security checks listed in paragraph 2.2; or

(ii) the Authority has given prior written permission for a named individual to perform a specific role.

2.2 For the purposes of paragraph 2.1, 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

(i) 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.

Annual training

2.3 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; and

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

Staff access

2.4 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.

2.5 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.

2.6 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.

Exception for certain Sub-contractors

2.7 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.

3 End-user Devices

3.1 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 processed in accordance the following requirements:

(a) the operating system and any applications that store, process 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 a 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 Suppler 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.

3.2 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.

3.3 Where there is any conflict between the requirements of this Schedule [x] and the requirements of the NCSC Device Guidance, the requirements of this Schedule take precedence.

4 Hardware and software support

4.1 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.

4.2 The Supplier must produce and maintain a register of all software that forms the Supplier Information Management System

Support Register

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

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

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

4.4 The Supplier must:

(a) review and update the Support Register:

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

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

(d) at least once every 12 months;

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

(ii) whenever it updates the Support Register; and

(i) otherwise when the Authority requests.

4.5 Where any element of the Developed 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.

4.6 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 Encryption

5.1 Before Processing any Authority Data, the Supplier must agree with the Authority the encryption methods that it and any Sub-contractors that Process Authority Data will use to comply with this paragraph 5.

5.2 Where this paragraph 5 requires Authority Data to be encrypted, the Supplier must use, and ensure that Subcontractors use, the methods agreed by the Authority under paragraph 5.1.

5.3 Unless paragraph 5.4 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.

5.4 Where the Supplier, or a Sub-contractor, cannot encrypt Authority Data as required by paragraph 5.2, 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.

5.5 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.

5.6 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.

5.7 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.

6 Email

6.1 Notwithstanding anything in the specification for the Developed System or this Contract, the Supplier must ensure that where the Developed System will provide an Email Service to the Authority, the Developed System:

(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).

7 DNS

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

8 Malicious Software

8.1 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.

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

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

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

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

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

(d) where Malicious Software has been introduced into the Supplier Information Management System, identifies, contains the spread of, and minimises the impact of Malicious Software.

8.4 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.

8.5 The Supplier must at all times, during and after the Term, on written demand indemnify the Authority and keep the Authority indemnified, against all Losses incurred by, awarded against or agreed to be paid by the Authority arising from 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 8.

9 Vulnerabilities

9.1 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”.

9.2 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 9.1.

9.3 For the purposes of this paragraph 9, 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.

10 Security testing

Responsibility for security testing

10.1 The Supplier is solely responsible for:

(a) the costs of conducting any security testing required by this paragraph 10 (unless the Authority gives notice under paragraph 10.2); and

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

Security tests by Authority

10.2 The Authority may, where it has significant concerns relating to the security of the Supplier Information Management System, give notice to the Supplier that the Authority will undertake the security testing required by paragraph 10.9.

10.3 Where the Authority gives notice under paragraph 10.2:

(a) the Supplier shall provide such reasonable co-operation as the Authority requests, including:

(i) such access to the Supplier Information Management System as the Authority may request; and

(ii) such technical and other information relating to the Information Management System as the Authority requests;

(b) the Authority must provide a full, unedited and unredacted copy of the report relating to the IT Health Check as soon as reasonably practicable after the Authority receives a copy of the report; and

(c) for the purposes of paragraphs 10.18 to 10.27:

(i) the Supplier must treat any IT Health Check commissioned by the Authority as if it were such a report commissioned by the Supplier; and

(ii) the time limits in paragraphs 10.18 and 10.20 run from the date on which the Authority provides the Supplier with the copy of the report under paragraph (b).

10.4 In addition to its rights under paragraph 10.2, the Authority and/or its authorised representatives may, at any time and without giving notice to the Supplier, carry out such tests (including penetration tests) as it may deem necessary in relation to:

(a) the Service;

(b) the Supplier Information Management System; and/or

(c) the Supplier's compliance with the Security Management Plan

Authority Security Tests

10.5 The Authority shall take reasonable steps to notify the Supplier prior to carrying out such Authority Security Tests to the extent that it is reasonably practicable for it to do so taking into account the nature of the Authority Security Tests.

10.6 The Authority shall notify the Supplier of the results of such Authority Security Tests after completion of each Authority Security Test.

10.7 The Authority shall design and implement the Authority Security Tests to minimise their impact on the delivery of the Services.

10.8 If an Authority Security Tests causes Supplier Non-Performance, the Authority Security Tests shall be treated as an Authority Cause, except where the root cause of the Supplier Non-Performance was a security-related weakness or vulnerability exposed by the Authority Security Tests.

Security tests by Supplier

10.9 The Supplier must:

(a) before submitting the draft Security Management Plan to the Authority for an Assurance Decision;

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

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

undertake the following activities:

(a) conduct security testing of the Supplier Information Management System, insofar as it relates to the Developed System but excluding the Development Environment (IT Health Check) in accordance with paragraph 10.15 to 10.17; and

(b) implement any findings, and remedy any vulnerabilities identified by the IT Health Check in accordance with paragraphs 10.18 to 10.27.

1.2 In addition to its obligations under paragraph 10.9, the Supplier must undertake any tests required by:

(a) any Remediation Action Plan;

(b) the ISO27001 Certification Requirements;

(c) Cyber Essentials Plus Certification Requirements;

(d) the Security Management Plan; and

(e) 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,

Supplier Security Test

1.3 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.

1.4 Where the Supplier fully complies with paragraph 10.11, 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.

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

1.6 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

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

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

(b) 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.

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

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

(e) agree with the Authority the scope, aim and timing of the IT Health Check.

1.8 The Supplier must commission the IT Health Check in accordance with the scope, aim and timing agreed by the Authority.

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

Remedying vulnerabilities

1.10 In addition to complying with paragraphs 10.20 to 10.27, 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 1 month of becoming aware of the vulnerability and its classification; and

(b) any vulnerabilities classified as medium in a Security Test report within 3 months of becoming aware of the vulnerability and its classification.

1.11 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 10.18.

Responding to a Security Test report

1.12 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**).

1.13 Where the Authority has commissioned a root cause analysis under paragraph 10.28, the Supplier shall ensure that the draft Remediation Action Plan addresses that analysis.

1.14 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.

1.15 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.

1.16 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 10.22 to 10.24 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 10.26 and 10.27.

1.17 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:

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

(b) 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

1.18 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.

1.19 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

1.20 Where:

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

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

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

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

(b) 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.

2 Access Control

2.1 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.

2.2 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;

(i) time limited; and

(ii) restrict the Privileged User's access to the internet.

2.3 The Supplier must ensure, and must ensure that all Sub-contractors ensure, that it logs all activity of the Privileged Users whenever those users access those accounts and keeps the activity logs for 20 Working Days before deletion.

2.4 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.

2.5 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.

3 Event logging and protective monitoring

Protective Monitoring System

3.1 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 or the Developed System

3.2 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

3.3 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

3.4 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

3.5 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.

4 Audit rights

Right of audit

4.1 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 [x] 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.

4.2 Any audit undertaken under this paragraph 13.1:

(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.

4.3 The Authority may not undertake more than one audit under paragraph 13.1 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 Security Breach 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

(i) a Breach of Security.

Conduct of audits

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

4.5 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.

4.6 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

4.7 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.

4.8 The exercise by the Authority of any rights it may have under this paragraph 3 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.

5 Breach of Security

Reporting Breach of Security

5.1 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

5.2 The Supplier must, upon becoming aware of a Breach of Security immediately take those steps identified in the Security Management Plan (if applicable) 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

5.3 As soon as reasonably practicable and, in any event, within 5 Working Days, or such other period agreed with the Authority, following the Breach of Security, 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 root cause of the Breach of Security

Breach Action Plan

5.4 The draft Breach Action Plan must, in respect of each issue identified in the root cause analysis:

(a) how the issue will be remedied;

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

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

5.5 The Supplier shall promptly provide the Authority with such technical and other information relating to the draft Breach Action Plan as the Authority requests.

5.6 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 submit a revised draft Breach Action Plan that takes into account the Authority's reasons; and

(ii) paragraph 14.5 and 14.6 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.

Assistance to Authority

5.7 Where the Breach of Security concerns or is connected with the Authority Data or the Code, the Supplier must provide such assistance to the Authority as the Authority requires until the Breach of Security and any impacts or potential impacts on the Authority are resolved to the Authority's satisfaction.

5.8 The obligation to provide assistance under paragraph 14.7 continues notwithstanding the expiry or termination of this Contract.

Reporting of Breach of Security to regulator

5.9 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

(i) 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.

5.10 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.

6 Exit management

6.1 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

6.2 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.

6.3 The Supplier shall comply with the provisions of the Data Migration Plan during Exit Management.

7 Return and deletion of Authority Data

7.1 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

7.2 The Supplier must:

(a) review and update the Authority Data Register:

(i) within ten Working Days of the Supplier or any Sub-contractor changes 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.

7.3 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.

7.4 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 code 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;

(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 Process 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 11.1 to 11.4 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 depository for the deployment pipeline, use only a cloud-based code depository 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 (**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 Process Authority Data where the licence terms of that software purport to grant the licensor rights to Process 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 The Supplier must produce and maintain a register of all Third-party Software Modules that form part of the Code (the "**Modules Register**").

7.3 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.

7.4 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 [Authority-led Assurance] of the Supplier Information Management System;

(d) [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 late than [five] Working Days before each meeting of the Security Working 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

Commercial Information Assurance Team

Security Management Plan Template [Project/Service and Supplier Name]

Dated 2023

Contents

Insert table of contents for Security Management Plan

APPENDICES

1 Executive summary

[*This section should contain a brief summary of the business context of the system, the assurance work done, any off-shoring considerations and any significant residual risks that need acceptance*.]

1.1 Change history

Version Number	Date of Change	Change made by	Nature and reason for change

1.2 References, links and dependencies

ID	Document Title	Reference	Date

1.3 Supplier personnel

Key Personnel Names	Title	Contact Details incl. Mobile Number and Email Address

2 System description

2.1 Background

[*A short description of the project/product/system. Describe its purpose, functionality, aim and scope*.]

2.2 Organisational Ownership/Structure

[*Who owns the system and operates the system and the organisational governance structure. This should include how any ongoing security management is integrated into the project governance eg how a Security Working Group reports to the project board*.]

2.3 Information assets and flows

(a) Logical data flow diagram

[*This should include a simple high level logical diagram on one page. The diagram must include any third party suppliers and the data flows to/from them.*]

(b) Data assets

[*Include a table of the type and volumes of data that will be processed, managed and stored within the supplier system. If personal data, please include the fields used such as name, address, department DOB, NI number etc. Data processed by third party suppliers must be included here*]

2.4 System architecture

[*A description of the physical system architecture, to include the system management. Please provide a diagram.*]

2.5 Users

[*Please provide a table of the system users, this should include all users including HMG users as well as any service provider users and system managers. If relevant, security clearance level requirements should be included.*]

2.6 Locations

[*Please provide a table of where the Authorities data assets are stored, processed and any locations they are managed from. This must include the locations of any help desks or call centres if relevant. All third party suppliers and subcontractors must be included in this section. Any off-shoring considerations should be detailed with the legal basis for the data transfer included eg Standard Contractual Clauses, equivalency etc.*]

2.7 Certifications

[*Please include a table of any independent security certifications (eg ISO 27001:2013, Cyber Essentials Plus and Cyber Essentials) held as required by the contract. The table should include any relevant third party suppliers or subcontractors and must include the expiry date of the certification. Copies of the certificates should be included in Appendix 1.*]

2.8 Test and development systems

[*Include information about any test, development and User Acceptance testing systems, their locations and whether they contain live system data.*]

2.9 Modules Register

[*If code development is being undertaken, include a table of all Third-party Software Modules that form part of the Code. This must include the name of the developer, the due diligence undertaken by the supplier, any recognised security vulnerabilities and how the supplier will minimise the effect of those.*]

2.10 Support Register

[*A table should be included of all software used in any development activity, including the date it will cease to be in mainstream support.*]

3 Risk assessment

3.1 Accreditation/assurance scope

[*This section should describe the scope of the Risk Assessment and should indicate the components of the architecture upon which reliance is placed but assurance will not be done eg a cloud hosting service or a SAAS product/tool. A logical diagram should be used along with a brief description of the components. This scope must be agreed by the Authority.*]

3.2 Risk appetite

[*A risk appetite should be provided by the Authority and included here.*]

3.3 Business impact assessment

[*A description of the information assets and the impact of their loss or corruption (eg large amounts of Official Sensitive personal data the loss of which would be severely damaging to individuals, embarrassing to HMG, and make HMG liable to ICO investigations) in business terms should be included. This section should cover the impact on loss of confidentiality, integrity and availability of the assets and should be agreed with the Authority. The format of this assessment may be dependent on the risk assessment method chosen.*]

3.4 Risk assessment

[*The content of this section will depend on the risk assessment methodology chosen, but should contain the output of the formal information risk assessment in a prioritised list using business language. Experts on the system and business process should have been involved in the risk assessment to ensure the formal risk methodology used has not missed out any risks. The example table below should be used as the format to identify the risks and document the controls used to mitigate those risks.*]

Risk ID	Inherent risk	Inherent risk level	Vulnerability	Controls	Residual risk level
R1	Internet attackers could hack the system.	Medium	The service systems are exposed to the internet via the web portal.	C1: Internet-facing firewalls C2: Internet-facing IP whitelist C3: System hardening C4: Protective monitoring C5: Application access control C16: Anti-virus for incoming files C54: Files deleted when processed C59: Removal of departmental identifier	Very low
R2	Remote attackers could intercept or disrupt information crossing the internet.	Medium	File sharing with organisations across the internet.	C9: TLS communications C10: PGP file-sharing	Very low

Risk ID	Inherent risk	Inherent risk level	Vulnerability	Controls	Residual risk level
R3	Internal users could maliciously or accidentally alter bank details.	Medium-High	Users bank details can be altered as part of the normal business function.	C12. System administrators hold SC clearance. C13. All changes to user information are logged and audited. C14. Letters are automatically sent to users home addresses when bank details are altered. C15. Staff awareness training	Low

3.5 Controls

[*The controls listed above to mitigate the risks identified should be detailed. There should be a description of each control, further information and configuration details where relevant, and an assessment of the implementation status of, and assurance in, the control. A sample layout is included below*.]

ID	Control title	Control description	Further information and assurance status
C1	Internet-facing firewalls	Internet-facing firewalls are in place between the internet and the system', which restrict access from the internet to the required ports only.	Assured via ITHC firewall rule check
C2	Internet-facing IP whitelist	An IP whitelist is in place for all access from the internet.	Assured via ITHC
C15	Staff awareness training	All staff must undertake annual security awareness training and this process is audited and monitored by line managers.	Assured as part of ISO27001 certification

3.6 Residual risks and actions

[*A summary of the residual risks which are likely to be above the risk appetite stated after all controls have been applied and verified should be listed with actions and timescales included*.]

4 In-service controls

[*This section should describe how the main security requirements as specified in the contract (security schedule) are met.*]

4.1 Protective monitoring

[*This section should describe how your protective monitoring arrangements identify anomalous behaviour and how this is then acted upon as well as how logging and auditing of user activity is done.*]

4.2 Malware prevention

[*This should describe how your anti-virus solution is implemented with respect to protecting Authority assets.*]

4.3 End user devices

[*This section should detail the security controls which are implemented on all fixed and removable end user devices used to process, store or manage Authority data against the end-user device requirements in this contract.*]

4.4 Encryption

[*This section should detail the encryption measures you employ to protect Authority data both in transit and at rest.*]

4.5 Vulnerability management

[*This section should detail your process for identifying, classifying, prioritising, remediating, and mitigating" software vulnerabilities within your IT environment.*]

4.6 Identity, verification and access controls

[*This section should detail your password policy, your approach to ensuring that privileged accounts are accessible only from end-user devices dedicated to that use and by authenticated named users. This should include your use of multi-factor authentication for all accounts that have access to Authority data as well as privileged accounts.*]

4.7 Data Deletion

[*This section should include the agreed process for securely deleting Authority data when required.*]

5 Supply chain security and third party subcontractors/tools

[*This section should detail the assurance process for managing any security risks from Subcontractors and Third Parties authorised by the Authority with access to Authority data.*]

6 Security requirements on participating departments, customers and users

[*Please detail any security requirements or codes of connection required by participating departments/agencies/third parties.*]

7 Personnel security

[*Please provide details of your Personnel Security Vetting Policy for those staff who will have access to, or come into contact with Buyer data or assets.*

Please provide details of how you will ensure that all staff accessing Buyer data are aware of the confidential nature of the data and comply with their legal and specific obligations under the Contract.]

8 Business continuity

[*Please provide an overview of your organisation's business continuity and disaster recovery plans in terms of the Buyer data under the Contract, or attach a copy of your Business Continuity Plan*.]

9 Physical security

[*Please provide details of the building where the service will operate from and describe the procedures and security in place to control access to premises and any areas holding Buyer assets. Detail measures such as construction of buildings used for handling Buyer assets, availability of lockable storage, procedures covering end of day/silent hours, key management, visitor controls.*

Please also include details of any automated access controls, alarms and CCTV coverage. Please also provide details of the maintenance schedule of these security controls.> For the locations where Authority assets are held please provide details of any procedures and security in place designed to control access to the site perimeter. Please detail the measures in place such as fencing, CCTV, guarding, and procedures and controls to handle staff and visitors requesting access to the site. Please also provide details of the maintenance schedule of your security controls.]

10 Major hardware and software and end of support dates

[*This should be a table which lists the end of support dates for hardware and software products and components. An example table is shown below.*]

Name	Version	End of mainstream Support/Extended Support	Notes/RAG Status
Server Host	Supplier name XXXX	Feb 2020/March 2022	

11 Incident management process

[*The suppliers' process, as agreed with the Authority/Customer, should be included here. It must as a minimum include the protocol for how and when incidents will be reported to the Authority/customer and the process that will be undertaken to mitigate the incidents and investigate the root cause*.]

12 Required changes register

[*The table below shows the headings for the Required Changes Register which should be maintained and used to update the contents of this document at least annually*.]

Ref	Section	Change	Agreed With	Date agreed	Documentation update	Status

1	6.4	A new Third Party supplier XXXX will be performing the print capability.	Authority name	11/11/2021	Jul-2022	Open

Appendix 1 - ISO27001 and/or cyber essential plus certificates

[*Please include copies of the certificates here*]

Appendix 2 - Cloud security principles assessment

[*Please add your controls in the attached table.*]

Principle	Goals of the Principle	Controls
Principle 1 – Data in transit protection "User data transiting networks should be adequately protected against tampering and eavesdropping."	● Data in transit is protected between end user device(s) and the service A Data in transit is protected internally within the service ● Data in transit is protected between the service and other services (eg where APIs are exposed)	
Principle 2 – Asset protection and resilience "User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure."	Cloud service consumers should seek to understand: ● In which countries their data will be stored, processed and managed. They should also consider how this affects compliance with relevant legislation eg Data Protection Act (DPA), GDPR etc. B Whether the legal jurisdiction(s) within which the service provider operates are acceptable to them	
Principle 3 – Separation between users "A malicious or compromised user of the service should not be able to affect the service or data of another."	Cloud service consumers should seek to: ● Understand the types of user they share the service or platform with C Have confidence that the service provides sufficient separation of their data and service	

Principle	Goals of the Principle	Controls
	from other users of the service ● Have confidence that management of their service is kept separate from other users (covered separately as part of Principle 9)	
Principle 4 – Governance framework "The service provider should have a security governance framework which coordinates and directs its management of the service and information within it. Any technical controls deployed outside of this framework will be fundamentally undermined."	Cloud service consumers should ensure that: ● A clearly identified, and named, board representative (or a person with the direct delegated authority) is responsible for the security of the cloud service. This is typically someone with the title 'Chief Security Officer', 'Chief Information Officer' or 'Chief Technical Officer' D A documented framework exists for security governance, with policies governing key aspects of information security relevant to the service ● Security and information security are part of the service provider's financial and operational risk reporting mechanisms, ensuring that the board would be kept informed of security and information risk E Processes to identify and ensure compliance with applicable legal and regulatory requirements have been established	

Principle	Goals of the Principle	Controls
Principle 5 – Operational security "The service needs to be operated and managed securely in order to impede, detect or prevent attacks. Good operational security should not require complex, bureaucratic, time consuming or expensive processes."	Cloud service consumers should be confident that: ● The status, location and configuration of service components (both hardware and software) are tracked throughout their lifetime F Changes to the service are assessed for potential security impact. Then managed and tracked through to completion	
Principle 6 – Personnel security "Where service provider personnel have access to your data and systems you need a high degree of confidence in their trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise by service provider personnel."	Cloud service consumers should be confident that: ● The level of security screening conducted on service provider staff with access to the consumers information, or with ability to affect the service, is appropriate G The minimum number of people necessary have access to the consumers information or could affect the service	
Principle 7 – Secure development "Services should be designed and developed to identify and mitigate threats to their security. Those which aren't may be vulnerable to security issues which could compromise your data, cause loss of service or enable other malicious activity."	Cloud service consumers should be confident that: ● New and evolving threats are reviewed, and the service improved in line with them H Development is carried out in line with industry good practice regarding secure design, coding, testing and deployment	

Principle	Goals of the Principle	Controls
	● Configuration management processes are in place to ensure the integrity of the solution through development, testing and deployment	
Principle 8 – Supply chain security "The service provider should ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement."	Cloud service consumers should seek to understand and accept: ● How their information is shared with, or accessible to, third party suppliers and their supply chains I How the service provider's procurement processes place security requirements on third party suppliers ● How the service provider manages security risks from third party suppliers J How the service provider manages the conformance of their suppliers with security requirements ● How the service provider verifies that hardware and software used in the service is genuine and has not been tampered with	
Principle 9 – Secure user management "Your provider should make the tools available for you to securely manage your use of their service. Management interfaces and procedures are a vital part of the security	Cloud service consumers should: ● Be aware of all of the mechanisms by which the service provider would accept management or support requests from you (telephone, web portal, email etc.)	

Principle	Goals of the Principle	Controls
barrier, preventing unauthorised access and alteration of your resources, applications and data."	K Ensure that only authorised individuals from their organisation can use those mechanisms to affect their use of the service (Principle 10 can help consumers consider the strength of user identification and authentication in each of these mechanisms)	
Principle 10 – Identity and authentication "All access to service interfaces should be constrained to authenticated and authorised individuals."	Cloud service consumers should: ● Have confidence that identity and authentication controls ensure users are authorised to access specific interfaces	
Principle 11 – External interface protection "All external or less trusted interfaces of the service should be identified and appropriately defended."	Cloud service consumers should: ● Understand what physical and logical interfaces their information is available from, and how access to their data is controlled L Have sufficient confidence that the service identifies and authenticates users to an appropriate level over those interfaces (see Principle 10)	
Principle 12 – Secure service administration "Systems used for administration of a cloud service will have highly privileged access to that service. Their	Cloud service consumers should: ● Understand which service administration model is being used by the service provider to manage the service	

Principle	Goals of the Principle	Controls
compromise would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data."	M Be content with any risks the service administration model in use brings to the consumers data or use of the service	
Principle 13 – Audit information for users "You should be provided with the audit records needed to monitor access to your service and the data held within it. The type of audit information available to you will have a direct impact on your ability to detect and respond to inappropriate or malicious activity within reasonable timescales."	Cloud service consumers should: ● Be aware of the audit information that will be provided, how and when it will be made available, the format of the data, and the retention period associated with it N Be confident that the audit information available will meet their needs for investigating misuse or incidents	
Principle 14 – Secure use of the service "The security of cloud services and the data held within them can be undermined if you use the service poorly. Consequently, you will have certain responsibilities when using the service in order for your data to be adequately protected."	Cloud service consumers should: ● Understand any service configuration options available to them and the security implications of their choices O Understand the security requirements of their use of the service ● Educate their staff using and managing the service in how to do so safely and securely	

Appendix 3 - Protecting bulk data assessment if required by the authority/customer

[*A spreadsheet may be attached*]

Appendix 4 - Latest ITHC report and vulnerability correction plan

Appendix 5 - Statement of applicability

[*This should be a completed ISO 27001:2013 Statement of Applicability for the Information Management System if ISO27001 certification is required by the contract*.]