1 Supplier obligations

1.1 Where the Buyer has assessed this Contract as a higher-risk agreement, the Supplier must comply with all requirements of this Schedule 16 (Security).

1.2 Where the Buyer has assessed this Contract as a standard risk agreement, the Supplier must comply with all requirements of this this Schedule 16 (Security) except:

(a) Paragraph 11 (*Security Management Plan*);

(b) Paragraph 9 of the Security Requirements (*Code Reviews*);

(c) Paragraph 11 of the Security Requirements (*Third-party Software Modules*);

(d) Paragraph 12 of the Security Requirements (*Hardware and software support*);

(e) Paragraph 13 of the Security Requirements (*Encryption*); and

(f) Paragraph 20 of the Security Requirements (*Access Control*).

1.3 Where the Buyer has not made an assessment in the table in Paragraph 1, the Parties must treat this Contract as a higher-risk agreement.

2 Definitions

2.1 In this Schedule 16 (Security):

"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;
"Backup and Recovery Plan"	the document setting out the Suppliers' and Sub-contractors' plans for the back and recovery of any Government Data they Handle;
"Breach Action Plan"	means a plan prepared under Paragraph 23.3 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 Buyer Premises, the Sites, the Supplier Information Management System and/or any information or data used by the Buyer, the Supplier or any Sub-contractor in connection with this Contract, including the Government Data and the Code; (b) the loss (physical or otherwise), corruption and/or unauthorised disclosure of any information or data, including copies of such information or data, used by the Buyer, the Supplier or any Sub-contractor in connection with this Contract, including the Government Data and the Code; and/or (c) any part of the Supplier Information Management System ceasing to be compliant with the Certification Requirements; (d) the installation of Malicious Software in the: (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;
"Buyer Equipment"	means any hardware, computer or telecoms devices, and equipment that forms part of the Buyer System;
"Certification Default"	means the occurrence of one or more of the circumstances listed in Paragraph 10.4;
"Certification Rectification Plan"	means the plan referred to in Paragraph 10.5(a);

"Certification Requirements"	means the requirements set out in Paragraph 10.3;
"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; (b) holds "Green Light" status; and (c) is authorised to provide the IT Health Check services required by Paragraph 19 of the Security Requirements;
CHECK Team Leader	means an individual with a CHECK Scheme team leader qualification issued by the NCSC;
CHECK Team Member	means an individual with a CHECK Scheme team member qualification issued by the NCSC;
"Code"	means, in respect of the Developed System: (a) the source code; (b) the object code; (c) third-party components, including third-party coding frameworks and libraries; and (d) 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 16 (Security*)*; and (ii) the Secure Development Guidance;
"Code Review Plan"	means the document agreed with the Buyer under Paragraph 9.3 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;
"Developed System"	means the software or system that the Supplier is required to develop under this Contract;
"Development Activity"	means any activity relating to the development, deployment maintenance and upgrading of the Developed System, including: (a) coding; (b) testing; (c) code storage; and (d) deployment;
"Development Environment"	means any information and communications technology system and the Sites 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 provided by the Supplier or a Sub-contractor and used in the provision of the Services;
"Email Service"	means a service that will send, or can be used to send, emails from the Buyer's email address or otherwise on behalf of the Buyer;
"Expected Behaviours"	means the expected behaviours set out and updated from time to time in the Government Security Classification Policy, currently found at paragraphs 12 to 16 and in the table below paragraph 16 of https://www.gov.uk/government/publications/government-security-classifications/guidance-11-working-at-official-html;
"Government Data Register"	means the register of all Government Data the Supplier, or any Sub-contractor, receives from or creates for the Buyer, produced and maintained in accordance with Paragraph 24 of the Security Requirements;
"Government Security Classification Policy"	means the policy, as updated from time to time, establishing an administrative system to protect information assets appropriately against prevalent threats, including classification tiers, protective security controls and baseline behaviours, the current version of which is found at https://www.gov.uk/government/publications/government-security-classifications;
"**Handle**"	means any operation performed on data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of that data;
"**Higher-risk Sub-contractor**"	means a Sub-contractor that Handles Authority Data that the Authority, in its discretion, has designated as a Higher-risk Sub-contractor;

"**HMG Baseline Personnel Security Standard**"	means the employment controls applied to any individual member of the Supplier Staff that performs any activity relating to the provision or management of the Services, as set out in "HMG Baseline Personnel Standard", Version 7.0, June 2024 (https://www.gov.uk/government/publications/government-baseline-personnel-security-standard), as that document is updated from time to time;
ISO Certification	means either of the following certifications when issued by a UKAS-recognised Certification Body: (a) ISO/IEC27001:2013, where the certification was obtained before November 2022, but only until November 2025; and (a) ISO/IEC27001:2022 in all other cases;
"**IT Health Check**"	means security testing of the Supplier Information Management System, insofar as it relates to the Developed System but excluding the Development Environment in accordance with Paragraph 19.2 of the Security Requirements;
"**Medium-risk Sub-contractor**"	means a Sub-contractor that Handles Authority Data that the Authority, in its discretion, has designated as a Higher-risk Sub-contractor;
"**Modules Register**"	means the register of Third-party Software Modules required for higher risk agreements by Paragraph 11.4 of the Security Requirements;
"**NCSC**"	means the National Cyber Security Centre;
"**NCSC Cloud Security Principles**"	means the NCSC's document "Implementing the Cloud Security Principles" as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles;
"**NCSC Device Guidance**"	means the NCSC's document "Device Security Guidance", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/device-security-guidance;
"**NCSC Protecting Bulk Personal Data Guidance**"	means the NCSC's document "Protecting Bulk Personal Data", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/protecting-bulk-personal-data;
"**NCSC Secure Design Principles"**	means the NCSC's document "Secure Design Principles", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cyber-security-design-principles/cyber-security-design-principles;
"**OWASP**"	means the Open Web Application Security Project Foundation;
"**OWASP Secure Coding Practice**"	means the Secure Coding Practices Quick Reference Guide published by OWASP, as updated or replaced from time to time and found at https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/;

"**OWASP Top Ten**"	means the list of the most critical security risks to web applications published annually by OWASP and found at https://owasp.org/www-project-top-ten/;
"**Privileged User**"	means a user with system administration access to the Supplier Information Management System, or substantially similar access privileges;
"**Prohibited Activity**"	means the storage, access or Handling of Government Data prohibited by a Prohibition Notice;
"**Prohibition Notice**"	means a notice issued under Paragraph 1.11 of the Security Requirements;
"**Protective Monitoring System**"	means the system implemented by the Supplier and its Sub-contractors under Paragraph 21.1 of the Security Requirements to monitor and analyse access to and use of the Supplier Information Management System, the Development Environment, the Government Data and the Code;
"Questionnaire Response"	means the Supplier's response to the Secure by Design Questionnaire;
"**Register of Support Locations and Third-party Tools**"	means document setting out, in respect of Support Locations and Third-party Tools: (a) the nature of the activity performed at the Support Location or by the Third-party Tool on the Code or the Government Data (as applicable); (b) where that activity is performed by individuals, the place or facility from where that activity is performed; and (c) in respect of the entity providing the Support Locations or Third-party Tools, its: (i) full legal name; (ii) trading name (if any) (iii) country of registration; (iv) registration number (if applicable); and (v) registered address;
"**Relevant Activities**"	means those activities specified in Paragraph 1 of the Security Requirements;
"**Relevant Certifications**"	means: (a) for the Supplier: (i) in the case of a higher-risk agreement (A) either:

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

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

(B) Cyber Essentials Plus;

(ii) in the case of a standard agreement, either:

(C) the certification selected by the Buyer in Paragraph 1; or

(D) where the Buyer has not selected a certification option, Cyber Essentials; and

(b) for Higher-risk Subcontractors and Medium-risk Sub-contractors, either:

(i) the certification selected by the Buyer in Paragraph 1; or

(ii) where the Buyer has not selected a certification option, Cyber Essentials,

(or equivalent certifications);

"**Relevant Convictions**"	means any previous or pending prosecution, conviction or caution (excluding any spent conviction under the Rehabilitation of Offenders Act 1974) relating to offences involving dishonesty, terrorism, immigration, firearms, fraud, forgery, tax evasion, offences against people (including sexual offences), or any other offences relevant to Services as the Buyer may specify;
"**Remediation Action Plan**"	means the plan prepared by the Supplier in accordance with Paragraph 19.14 to 19.18, addressing the vulnerabilities and findings in a IT Health Check report;
Remote Location	means a location other than a Supplier's or a Sub-contractor's Site;
Remote Working	means the provision or management of the Services by Supplier Staff from a location other than a Supplier's or a Sub-contractor's Site;
Remote Working Policy	the policy prepared and approved under Paragraph 3 of the Security Requirements under which Supplier Staff are permitted to undertake Remote Working;
Secure by Design Approach	means the Secure by Design policy issued by the Cabinet Office as updated or replaced from time to time, currently found at: https://www.security.gov.uk/policy-and-guidance/secure-by-design/principles/;

Secure by Design Principles	means the Secure by Design Principles issued by the Cabinet Office, as updated or replaced from time-to-time, currently found at https://www.security.gov.uk/guidance/secure-by-design/activities/tracking-secure-by-design-progress;
Secure by Design Questionnaire	the questionnaire in Annex 3 (*Secure by Design Questionnaire*), implementing the Secure by Design Principles issued by the Cabinet Office, as updated or replaced from time to time, currently found at https://www.security.gov.uk/policy-and-guidance/secure-by-design/activities/tracking-secure-by-design-progress/;
"**Secure Development Guidance**"	means: (a) the NCSC's document "Secure development and deployment guidance" as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/developers-collection; and (b) the OWASP Secure Coding Practice as updated or replaced from time to time;
"**Security Management Plan**"	means the document prepared in accordance with the requirements of Paragraph 11 and in the format, and containing the information, specified in Annex 2;
"**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 (b) 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;
"**Sub-contractor**"	means, for the purposes of this Schedule 16 (Security) only, any individual or entity that: (a) forms part of the supply chain of the Supplier; and (b) has access to, hosts, or performs any operation on or in respect of the Supplier Information Management System, the Development Environment, the Code and the Government Data, and this definition shall apply to this Schedule 16 in place of the definition of Sub-Contractor in Schedule 1 *(Definitions)*.
"**Sub-contractor Staff**"	means: (a) any individual engaged, directly or indirectly, or employed, by any Sub-contractor; and (b) 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;

"**Supplier Information Management System**"	means: (a) those parts of the information and communications technology system and the Sites that the Supplier or its Sub-contractors will use to provide the Services; (b) the associated information assets and systems (including organisational structure, controls, policies, practices, procedures, processes and resources); and (c) for the avoidance of doubt includes the Development Environment;
"**Security Requirements**"	mean the security requirements in Annex 1 to this Schedule ♦16] (Security *Management*);
"**Support Location**"	means a place or facility where or from which individuals may access or Handle the Code or the Government Data;
"**Support Register**"	means the register of all hardware and software used to provide the Services produced and maintained for Higher Risk Contracts in accordance with Paragraph 12 of the Security Requirements;
"**Third-party Software Module**"	means any module, library or framework that: (d) is not produced by the Supplier or a Sub-contractor as part of the Development Activity; and (e) 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 Software used by the Supplier by which the Code or the Government Data is accessed, analysed or modified or some form of operation is performed on it;
"**UKAS**"	means the United Kingdom Accreditation Service;
"**UKAS-recognised Certification Body**"	means: (a) an organisation accredited by UKAS to provide certification of ISO/IEC27001:2013 and/or ISO/IEC27001:2022; or (b) an organisation accredited to provide certification of ISO/IEC27001:2013 and/or ISO/IEC27001:2022 by a body with the equivalent functions as UKAS in a state with which the UK has a mutual recognition agreement recognising the technical equivalence of accredited conformity assessment.

3 Introduction

3.1 This Schedule 16 (Security) sets out:

(a) the assessment of this Contract as either a:

(i) higher risk agreement; or

(ii) standard agreement,

in Paragraph 1;

(b) the arrangements the Supplier must implement before, and comply with when, providing the Services and performing its other obligations under this Contract to ensure the security of:

(i) the Development Activity;

(ii) the Development Environment;

(iii) the Government Data;

(iv) the Services; and

(v) the Supplier Information Management System;

(c) the principle of co-operation between the Supplier and the Buyer on security matters, in Paragraph 5;

(d) the Buyer's access to the Supplier Staff and Supplier Information Management System, in Paragraph 8;

(e) the Certification Requirements, in Paragraph 10;

(f) the requirements for a Security Management Plan in the case of higher-risk agreements, in Paragraph 11; and

(g) the Security Requirements with which the Supplier and its Sub-contractors must comply.

4 Principles of Security

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

(a) the Buyer System;

(b) the Supplier System;

(c) the Sites;

(d) the Services; and

(e) the Supplier's Information Management System.

4.2 The Parties shall share information and act in a co-operative manner at all times to further the principles of security in Paragraph 5.1.

4.3 Notwithstanding the involvement of the Buyer in the assurance of the Supplier Information Management System, the Supplier remains responsible for:

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

(b) the security and integrity of the Developed System; and

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

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

5 Security Requirements

5.1 The Supplier shall:

(a) comply with the Security Requirements; and

(b) where the relevant option in Paragraph 1 is selected, comply with the Buyer Security Policies;

(c) ensure that all Sub-contractors comply with:

(i) the Security Requirements; and

(ii) where the relevant option in Paragraph 1 is selected, the Buyer Security Policies,

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

(iii) Paragraph 6.2 applies; or

(iv) the table in Annex 3 limits the Security Requirements that apply to a Sub-contractor; and

(d) where the Buyer has assessed this Contract as a higher-risk agreement, ensure at all times that its provision of the Services and its operation and management of the Supplier Information Management System complies with the Security Management Plan.

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

(a) use reasonable endeavours to ensure that the SMP Sub-contractor complies with all obligations this Schedule 16 (Security) imposes on Sub-contractors, including the Security Requirements;

(b) document the differences between those requirements 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 Staff

6.1 The Supplier must ensure that it all times it maintains within the Supplier Staff sufficient numbers of qualified, skilled security professionals to ensure the Supplier complies with the requirements of this Schedule 16 (Security).

6.2 The Supplier must appoint:

(a) a senior individual within its organisation with accountability for managing security risks and the Supplier's implementation of the requirements of this Schedule 16 (Security); and

(b) a senior individual within the team responsible for the delivery of the Services with responsibility for managing the security risks to the Supplier Information Management System.

6.3 The individuals appointed under Paragraph 7.2:

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

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

6.4 The Supplier must review, and if necessary replace, the individuals appointed under Paragraph 7.2 if required to do so by the Buyer.

7 Access to Supplier Staff and Supplier Information Management System

7.1 The Buyer may require, and the Supplier must provide, and ensure that each Sub-contractor provides, the Buyer and its authorised representatives with:

(a) access to the Supplier Staff, including, for the avoidance of doubt, the Sub-contractor Staff;

(b) access to the Supplier Information Management System, including those parts of the Supplier Information Management System under the control of, or operated by, any Sub-contractor; and

(c) such other information and/or documentation that the Buyer or its authorised representatives may require,

to allow the Buyer to audit the Supplier and its Sub-contractors' compliance with this Schedule 16 (Security) and the Security Requirements.

7.2 The Supplier must provide the access required by the Buyer in accordance with Paragraph 8.1:

(a) in the case of a Breach of Security within 24 hours of such a request; and

(b) in all other cases, within 10 Working Days of such request.

8 Government Data Handled using Supplier Information Management System

8.1 The Supplier acknowledges that the Supplier Information Management System:

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

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

in each case using the Government Security Classification Policy.

8.2 The Supplier must:

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

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

(i) immediately inform the Buyer; and

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

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

(a) the Expected Behaviours; and

(b) the Security Controls.

8.4 Where there is a conflict between the Expected Behaviours or the Security Controls and this Schedule 16 (Security) the provisions of this Schedule 16 (Security) shall apply to the extent of any conflict.

9 Certification Requirements

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

(a) it; and

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

is certified as compliant with the Relevant Certifications

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

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

(b) in the case of a higher-risk agreement, the any relevant scope and statement of applicability required under the ISO Certifications.

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

(a) currently in effect;

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

(c) are not subject to any condition that may impact the provision of the Services or the Development Activity (the "**Certification Requirements**").

9.4 The Supplier must notify the Buyer promptly, and in any event within three (3) Working Days, after becoming aware that, in respect of it or any Sub-contractor:

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

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

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

(d) the body that awarded a Relevant Certification has made it subject to conditions, the compliance with which may impact the provision of the Services

(each a "**Certification Default**").

9.5 Where the Supplier has notified the Buyer of a Certification Default under Paragraph 10.4:

(a) the Supplier must, within 10 Working Days of the date in which the Supplier provided notice under Paragraph 10.4 (or such other period as the Parties may agree) provide a draft plan (a "**Certification Rectification Plan**") to the Buyer 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 Buyer must notify the Supplier as soon as reasonably practicable whether it accepts or rejects the Certification Rectification Plan;

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

(d) the rejection by the Buyer 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.

10 Security Management Plan

10.1 This Paragraph 11 applies only where the Buyer has assessed that this Contract is a higher-risk agreement.

Preparation of Security Management Plan

10.2 The Supplier shall document in the Security Management Plan how the Supplier and its Sub-contractors shall comply with the requirements set out in this Schedule 16 (Security) and the Contract in order to ensure the security of the Development Environment, the Developed System, the Government Data and the Supplier Information Management System.

10.3 The Supplier shall prepare and submit to the Buyer within 20 Working Days of the date of this Contract, the Security Management Plan, which must include:

(a) an assessment of the Supplier Information Management System against the requirements of this Schedule 16 (Security), including the Security Requirements;

(b) 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 Development Environment, the Developed System. the Government Data, the Buyer, the Services and/or users of the Services; and

(c) 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);

(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 Development Activity undertaken by the Sub-contractor;

(v) the access the Sub-contractor has to the Development Environment;

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

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

(viii) the measures the Sub-contractor has in place to comply with the requirements of this Schedule 16 (Security);

(d) the Register of Support Locations and Third-party Tools;

(e) the Modules Register;

(f) the Support Register;

(g) details of the steps taken to comply with:

(i) the Secure Development Guidance; and

(ii) the secure development policy required by the ISO/IEC 27001:2022 Relevant Certifications;

(h) details of the protective monitoring that the Supplier will undertake in accordance with Paragraph 21 of the Security Requirements, including:

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

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

Approval of Security Management Plan

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

(a) an information security approval statement, which shall confirm that the Supplier may use the Supplier Information Management System to:

(i) undertake the Development Activity; and/or

(ii) Handle Government Data; or

(b) a rejection notice, which shall set out the Buyer's reasons for rejecting the Security Management Plan.

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

10.6 The process set out in Paragraph 11.5 shall be repeated until such time as the Authority issues a Risk Management Approval Statement to the Supplier or terminates this Contract.

10.7 The rejection by the Buyer of a second revised Certification Rectification Plan is a material Default of this Contract.

Updating Security Management Plan

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

Monitoring

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

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

(b) a new risk to the components or architecture of the Supplier Information Management System;

(c) a vulnerability to the components or architecture of the Supplier Information Management System using an industry standard vulnerability scoring mechanism;

(d) a change in the threat profile;

(e) a significant change to any risk component;

(f) a significant change in the quantity of Personal Data held within the Service;

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

(h) an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns.

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

11 Secure by Design Questionnaire

11.1 This Paragraph 12 applies only when the Buyer has selected the relevant option in Paragraph 1.

11.2 The Supplier must complete, by the date and in the format specified by the Buyer, and keep updated the Secure by Design Questionnaire

11.3 The Supplier must provide any explanations or supporting documents required by the Buyer to verify the contents of the Questionnaire Response.

11.4 The Supplier must ensure that at all times it provides the Services and operates and manages the Supplier System in the manner set out in its Questionnaire Response.

11.5 Where, at any time, the Buyer reasonably considers the Supplier's Questionnaire Responses do not, or do not adequately demonstrate the Supplier's compliance with:

(a) this Schedule;

(b) the Secure by Design Approach;

(c) the Security Management Plan (where applicable); or

(d) any applicable Buyer Security Policies,

the Supplier must, at its own costs and expense and by the date specified by the Buyer:

(e) update the Supplier System to remedy the areas of non-compliance identified by the Buyer;

(f) update the Questionnaire Responses to reflect the changes to the Supplier System; and

(g) re-submit the Questionnaire Responses to the Buyer.

11.6 Where the Supplier considers that there is an inconsistency between the explicit or implicit requirements of the Secure by Design Questionnaire and the requirements of this Schedule 16 (Security), the Supplier must:

(a) immediately inform the Buyer; and

(b) comply with any instructions from the Buyer to resolve the inconsistency.

11.7 Where the instructions from the Buyer have the effect of imposing additional or different requirements on the Supplier than the requirements of this Schedule 16 (Security):

(a) the Parties must agree an appropriate Contract Change to amend this Schedule; and

(b) until the agreement of that Contract Change, any inconsistency must be resolved by applying the documents in the following order of precedence:

(i) the requirements of this Schedule 16 (Security);

(ii) the Secure by Design Questionnaire; and

(iii) the Buyer Security Policies.

12 Withholding of Charges

12.1 The Buyer may withhold some or all of the Charges in accordance with the provisions of this Paragraph 13 where:

(a) the Supplier in in material Default of any of its obligations under this Schedule 16 (Security); 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 16 (Security)):

(i) a Notifiable Default;

(ii) an Intervention Cause; or

(iii) a Step-In Trigger Event.

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

12.3 Before withholding any Charges under Paragraph 13.1 the Buyer must

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

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

(ii) the amount of the Charges that the Buyer 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 Buyer will withhold the Charges; and

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

12.4 Where the Supplier does not remedy the Default by the date specified in the notice given under Paragraph 13.3(a), the Buyer may retain the withheld amount.

12.5 The Supplier acknowledges:

(a) the legitimate interest that the Buyer has in ensuring the security of the Supplier Information Management System and the Government Data and, as a consequence, the performance by the Supplier of its obligations under this Schedule 16 (Security); and

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

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

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

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

(a) withhold any Charges under Paragraph 13.1; or

(b) retain any Charges under Paragraph 13.4.

12.7 Any Dispute raised by the Supplier does not prevent the Buyer withholding Charges in respect of:

(a) the decision subject to the Dispute; or

(b) any other matter to which this Paragraph 13 applies.

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

12.9 The Buyer's right to withhold or retain any amount under this Paragraph 13 are in addition to any other rights that the Buyer may have under this Contract or in Law, including any right to claim damages for Losses it suffers arising from the Default.

Annex 1 Security Requirements

1 Location

Location for Relevant Activities

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

(a) undertake the Development Activity;

(b) host the Development Environment; and

(c) store, access or Handle Government Data,

(the "**Relevant Activities**") only in the geographic areas permitted by the Buyer in Paragraph 1.

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

(a) the United Kingdom; or

(b) a territory permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State).

1.3 The Supplier must, and must ensure 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 at least an onerous as those relating to Sub-contractors in this Schedule 16 (Security);

(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 Buyer with such information as the Buyer requires concerning:

(i) the entity;

(ii) the arrangements with the entity; and

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

(e) the Buyer has not given the Supplier a Prohibition Notice under Paragraph 1.11.

1.4 Where the Supplier cannot comply with one or more of the requirements of Paragraph 1.3:

(a) it must provide the Buyer with such information as the Buyer 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 Buyer may grant approval to use that location or those locations, and that approval may include conditions; and

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

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

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

Support Locations

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

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

(a) the United Kingdom; or

(b) a territory permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State).

1.7 the Supplier must, and must ensure 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) that binding agreement includes obligations on the entity in relation to security management equivalent to those relating to Sub-contractors in this Schedule 16 (Security);

(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 Buyer with such information as the Buyer requires concerning:

(i) the entity;

(ii) the arrangements with the entity; and

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

(e) the Buyer has not given the Supplier a Prohibition Notice under Paragraph 1.11.

Third-party Tools

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

(a) enter into a binding agreement with the provider of the Third-party Tool;

(b) the binding agreement includes obligations on the provider in relation to security management equivalent to those relating to Sub-contractors in this Schedule 16 (Security);

(c) take reasonable steps to assure itself that the provider complies with the binding agreement;

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

(e) the Supplier has provided the Buyer with such information as the Buyer requires concerning:

(i) the provider;

(ii) the arrangements with the provider; and

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

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

(f) the Buyer has not given the Supplier a Prohibition Notice under Paragraph 1.11.

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

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

(c) 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

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

Prohibited Activities

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

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

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

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

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

(b) use any specified Third-party Tool,

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

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

(a) undertakes any Prohibited Activities;

(b) uses any Support Locations;

(c) or employs any Third-party Tool,

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 Physical Security

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

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

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

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

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

(ii) adopts a layered approach to physical security;

(iii) has sections dealing with the following matters:

(A) the permitter of the Secure Location;

(B) the building fabric;

(C) security guarding;

(D) visitor and people management;

(E) server and communications rooms;

(F) protection of sensitive data;

(G) closed circuit television;

(H) automated access and control systems;

(I) intruder detection; and

(J) security control rooms.

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

3 Vetting, Training and Staff Access

Vetting before performing or managing Services

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

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

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

3.2 For the purposes of Paragraph 3.1, the security checks are:

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

(i) the individual's identity;

(ii) the individual's nationality and immigration status so as to demonstrate that they have a right to work in the United Kingdom;

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

(iv) that the individual has no Relevant Convictions;

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

(c) such other checks for the Supplier Staff of Sub-contractors as the Buyer may specify.

Exception for certain Sub-contractors

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

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

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

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

Annual training

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

(a) General training concerning security and data handling; and

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

(c) the Secure by Design Principles.

Staff access

3.5 The Supplier must ensure, and ensure that Sub-contractors ensure, that individual Supplier Staff can access only the Government Data necessary to allow individuals to perform their role and fulfil their responsibilities in the provision of the Services.

3.6 The Supplier must ensure, and ensure that Sub-contractors ensure, that where individual Supplier Staff no longer require access to the Government Data or any part of the Government Data, their access to the Government Data or that part of the Government Data is revoked immediately when their requirement to access Government Data ceases.

3.7 Where requested by the Buyer, the Supplier must remove, and must ensure that Sub-contractors remove, an individual Supplier Staff's access to the Government Data, or part of that Government Data specified by the Buyer, as soon as practicable and in any event within 24 hours of the request.

Remote Working

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(a) approve the proposed Remote Working Policy, in which case the Supplier must, and ensure that any applicable Sub-contractor, implements the approved Remote Working Plan in accordance with its terms;

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

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

(ii) the Supplier may:

(A) revise the proposed Remote Working Plan; and

(B) re-submit the proposed Remote Working Plan to the Buyer for approval under Paragraph 3.11.

4 End-user Devices

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

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

(b) users must authenticate before gaining access;

(c) all Government Data and Code must be encrypted using a encryption tool agreed to by the Buyer;

(d) the End-under 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 Government Data and Code to ensure the security of that Government 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 Government Data or Code stored on the device and prevent any user or group of users from accessing the device;

(g) all End-user Devices are within the scope of any Relevant Certification.

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

4.3 Where there any conflict between the requirements of this Schedule 16 (Security) and the requirements of the NCSC Device Guidance, the requirements of this Schedule take precedence.

5 Secure Architecture

5.1 The Supplier shall design and build the Developed System in a manner consistent with:

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

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

(c) the NCSC's guidance on "Cloud Security Principles".

5.2 Where any of the documents referred to in Paragraph 5.1 provides for various options, the Supplier must document the option it has chosen to implement and its reasons for doing so.

5.3 Notwithstanding anything in the specification for the Developed System or this Contract, the Supplier must ensure that the Developed System encrypts Government Data:

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

(b) when the Government Data is transmitted.

5.4 The Supplier must ensure that the Developed System is developed and configured so as to provide for the matters set out in Paragraphs 20.2 to 20.5 of the Security Requirements.

6 Secure Software Development by Design

6.1 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; and

(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.

6.2 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.

6.3 In particular, the Supplier must, and ensure that all Sub-contractors engaged in Development Activity:

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

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

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

(b) ensure that all Code:

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

(ii) follows OWASP Secure Coding Practice

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

(iv) employs consistent naming conventions;

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

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

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

(A) any original coding; and

(B) at any time the Code is changed;

(c) ensure that all Development Environments:

(i) protect access credentials and secret keys;

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

(iii) requires multi-factor authentication to access;

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

(v) use network architecture controls to constrain access from the Development Environment to the Developed System or the Supplier Information Management System.

6.4 The Supplier must, and must ensure that all Sub contractors engaged in Development Activity, incorporate into the Developed System any security requirements identified:

(a) during any user research concerning the Developed System; or

(b) identified in any business case, or similar document, provided by the Buyer to the Supplier to inform its Development Activity.

7 Code Repository and Deployment Pipeline

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

7.1 when using a cloud-based code repository for the deployment pipeline, use only a cloud-based code repository that has been assessed against the NCSC Cloud Security Principles;

7.2 ensure user access to cope repositories is authenticated using credentials, with passwords or private keys;

7.3 ensure secret credentials are separated from source code.

7.4 run automatic security testing as part of any deployment of the Developed System.

8 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.

9 Code Reviews

9.1 This Paragraph applies where the Buyer has assessed that this Contract is a higher-risk agreement.

9.2 The Supplier must:

(a) regularly; or

(b) as required by the Buyer

review the Code in accordance with the requirements of this Paragraph 9 (a "**Code Review**").

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

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

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

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

(d) the frequency of any Code Reviews,

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

9.4 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.

9.5 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.

9.6 No later than 10 Working Days after each Code Review, the Supplier must provide the Buyer will a full, unedited and unredacted copy of the Code Review Report.

9.7 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 Buyer with such information as it requests about the steps the Supplier takes under this Paragraph 9.7.

10 Third-party Software

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

11 Third-party Software Modules

11.1 This Paragraph 11 applies only where the Buyer has assessed that this Contract is a higher-risk agreement

11.2 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.

11.3 For the purposes of Paragraph 11.2(b), the Supplier must perform due diligence that is proportionate to the significance of the Third-party Software Module within the Code.

11.4 The Supplier must produce and maintain a register of all Third-party Software Modules that form part of the Code (the "**Modules Register**").

11.5 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.

11.6 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 6 (six) months;

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

(i) whenever it updates the Modules Register; and

(ii) otherwise when the Buyer requests.

12 Hardware and software support

12.1 This Paragraph 12 applies only where the Buyer has assessed that this Contract is a higher-risk agreement

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

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

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

(i) remedy vulnerabilities; or

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

12.3 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.

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

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

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

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

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

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

12.6 The Supplier must:

(a) review and update the Support Register:

(i) within 10 Working days of becoming aware of any new vulnerability in any item of software;

(ii) within 10 Working Days of becoming aware of the date on which, or any change to the date on which, any item of software will cease to be in mainstream security report;

(iii) within 10 Working Days of introducing new software, or removing existing software, from the Supplier Information Management System; and

(iv) at least once every 12 months;

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

(i) whenever it updates the Support Register; and

(ii) otherwise when the Buyer requests.

12.7 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.

12.8 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.

12.9 The Supplier must ensure that where any software or hardware component of the Supplier Information Management System is no longer required to provide the Services or has reached the end of its life it is removed or disconnected from the Supplier Information Management System.

13 Encryption

13.1 This Paragraph applies where the Buyer has assessed that this Contract is a higher-risk agreement.

13.2 Before Handling any Government Data, the Supplier must agree with the Buyer the encryption methods that it and any Sub-contractors that Handle Government Data will use to comply with this Paragraph 13.

13.3 Where this Paragraph 13 requires Government Data to be encrypted, the Supplier must use, and ensure that Subcontractors use, the methods agreed by the Buyer under Paragraph 13.2.

13.4 Notwithstanding anything in the specification for the Developed System or this Contract, the Supplier must ensure that the Developed System encrypts Government Data:

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

(b) when the Government Data is transmitted.

13.5 Unless Paragraph 13.6 applies, the Supplier must ensure, and must ensure that all Sub-contractors ensure, that Government 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.

13.6 Where the Supplier, or a Sub-contractor, cannot encrypt Government Data as required by Paragraph 13.5, the Supplier must:

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

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

(c) provide the Buyer with such information relating to the Government Data concerned, the reasons why that Government Data cannot be encrypted and the proposed protective measures as the Buyer may require.

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

13.8 Where the Buyer and Supplier reach agreement, the Supplier must document:

(a) the subset or subsets of Government 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 Government Data.

13.9 Where the Buyer and Supplier do not reach agreement within 40 Working Days of the date on which the Supplier first notified the Buyer that it could not encrypt certain Government Data, either party may refer the matter to [be determined by an expert in accordance with the Dispute Resolution Procedure].

14 Backup and recovery of Government Data

Backups and recovery of Government Data

14.1 The Supplier must backup and recover the Government Data in accordance with the Backup and Recovery Plan to ensure the recovery point objective and recovery time objective in Paragraph 14.3(a).

14.2 Any backup system operated by the Supplier or Sub-contractor forms part of the Supplier System or that Sub-contractor's System to which this Schedule 16 (Security) and the Security Requirements apply.

Backup and Recovery Plan

14.3 Unless otherwise required by the Buyer, the Backup and Recovery Plan must provide for:

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

(i) a recovery time objective of [**insert period**]; and

(ii) a recovery point objective of [**insert period**]; and

(b) a retention period of [**insert period**].

14.4 In doing so, the Backup and Recovery Plan must ensure that in respect of any backup system operated by the Supplier or a Sub-contractor:

(a) the backup location for Government Data is sufficiently physically and logically separate from the rest of the Supplier System or a Sub-contractor's System that it is not affected by any Disaster affecting the rest of the Supplier System or a Sub-contractor's System;

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

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

(d) newer backups of Government Data do not overwrite existing backups made during the retention period specified in Paragraph 14.3(a)(ii);

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

(i) identifies any backup failure; and

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

(f) any backup failure is remedied promptly;

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

(i) identify any recovery failure;

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

(h) any recovery failure is promptly remedied.

15 Email

15.1 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 Buyer, 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).

16 DNS

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

17 Malicious Software

17.1 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.

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

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

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

(c) provides for all updates to be the Anti-virus Software to be deployed within 10 Working Days of the update's release by the vendor;

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

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

17.3 If Malicious Software is found, the Parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Government Data, assist each other to mitigate any [Losses] and to restore the Services to their desired operating efficiency.

17.4 Any Breach of Security caused by Malicious Software where the Breach of Security arose from a failure by the Supplier, or a Sub-contractor, to comply with this Paragraph 17 is a material Default.

18 Vulnerabilities

18.1 Unless the Buyer otherwise agrees, the Supplier must ensure that it or any relevant Sub-contractor applies security patches to any vulnerabilities in the Supplier Information Management System no later than:

(a) seven (7) days after the public release of patches for vulnerabilities classified as "critical";

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

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

18.2 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 18.1.

18.3 For the purposes of this Paragraph 18, 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.

19 Security testing

Responsibility for security testing

19.1 The Supplier is solely responsible for:

(a) the costs of conducting any security testing required by this Paragraph 19; and

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

Security tests by Supplier

19.2 The Supplier must:

(a) during the testing of the Developed System and before the Developed System goes live;

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

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

undertake the following activities:

(d) conduct security testing of the Supplier Information Management System, insofar as it relates to the Developed System but excluding the Development Environment (an “**IT Health Check**”) in accordance with Paragraph 19.8 to 19.10; and

(e) implement any findings, and remedy any vulnerabilities identified by the IT Health Check in accordance with Paragraph and 19.11 to 19.20.

19.3 In addition to its obligations under Paragraph 19.2, the Supplier must undertake any tests required by:

(a) any Remediation Action Plan;

(b) the ISO27001 Certification Requirements;

(c) the Security Management Plan; and

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

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

19.4 The Supplier must:

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

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

19.5 Where the Supplier fully complies with Paragraph 19.4, if a Supplier Security Test causes a Performance Failure in a particular Measurement Period, the Supplier shall be entitled to relief in respect of such Performance Failure for that Measurement Period.

19.6 The Buyer may send a representative to witness the conduct of the Supplier Security Tests.

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

IT Health Checks

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

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

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

(c) design and plan for the IT Health Check so as to minimise the impact of the IT Health Check on the Supplier Information Management System and the delivery of the Services.

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

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

(f) agree with the Buyer the scope, aim and timing of the IT Health Check.

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

19.10 Following completion of an IT Health Check, the Supplier must provide the Buyer with a full, unedited and unredacted copy of the report relating to the IT Health Check without delay and in any event within 10 Working Days of its receipt by the Supplier.

Remedying vulnerabilities

19.11 In addition to complying with Paragraphs 19.13 to 19.20., the Supplier must remedy:

(a) any vulnerabilities classified as critical in the IT Health Check report within 5 Working Days of becoming aware of the vulnerability and its classification;

(b) any vulnerabilities classified as high in the IT Health Check report within 1 month of becoming aware of the vulnerability and its classification; and

(c) any vulnerabilities classified as medium in the IT Health Check report within 3 months of becoming aware of the vulnerability and its classification.

19.12 The Supplier must notify the Buyer immediately if it does not, or considers it will not be able to, remedy the vulnerabilities classified as critical, high or medium in the IT Health Check report within the time periods specified in Paragraph 19.11.

Significant vulnerabilities

19.13 Where the IT Health Check report identifies more than 10 vulnerabilities classified as either critical or high, the Buyer may, at the Supplier's cost, appoint an independent and appropriately qualified and experienced security architect and adviser to perform a root cause analysis of the identified vulnerabilities.

Responding to Supplier Security Test report

19.14 Where the IT Health Check identifies vulnerabilities in, or makes findings in respect of, the Information Management System, the Supplier must within 20 Working Days of receiving the IT Health Check report, prepare and submit for approval to the Buyer a draft plan addressing the vulnerabilities and findings (the "**Remediation Action Plan**").

19.15 Where the Buyer has commissioned a root cause analysis under Paragraph 19.13, the Supplier shall ensure that the draft Remediation Action Plan addresses that analysis.

19.16 The draft Remediation Action Plan must, in respect of each vulnerability identified or finding made by the IT Health Check 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.

19.17 The Supplier shall promptly provide the Buyer with such technical and other information relating to the Supplier Information Management System, the IT Health Check report or the draft Remediation Action Plan as the Buyer requests.

19.18 The Buyer 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 10 Working Days of the date on which the Buyer rejected the draft Remediation Action Plan submit a revised draft Remediation Action Plan that takes into account the Buyer's reasons; and

(ii) Paragraph 19.16 to 19.18 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 19.19 and 19.20.

Implementing an approved Remediation Action Plan

19.19 In implementing the Remediation Action plan, the Supplier must conduct such further tests on the Supplier Information Management System as are required by the Remediation Action Plan to confirm that the Remediation Action Plan has fully and correctly implemented.

19.20 If any such testing identifies a new risk, new threat, vulnerability or exploitation technique with the potential to affect the security of the Supplier Information Management System, the Supplier shall within [2] Working Days of becoming aware of such risk, threat, vulnerability or exploitation technique:

(a) provide the Buyer 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 Buyer.

Significant vulnerabilities

19.21 Where:

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

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

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

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

(d) give notice to the Supplier requiring the appointment as soon as reasonably practicable, and in any event within ten Working Days, of an Independent Security Adviser.

20 Access Control

20.1 This Paragraph applies where the Buyer has assessed that this Contract is a higher-risk agreement.

20.2 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 Government 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 Buyer on request.

20.3 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) in the case of a higher-risk agreement are:

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

(ii) time limited; and

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

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

20.5 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.

20.6 The Supplier must ensure that the Developed System is developed and configured so as to provide for the matters set out in Paragraphs 20.2 to 20.5.

20.7 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.

21 Event logging and protective monitoring

Protective Monitoring System

21.1 The Supplier must, and must ensure that Sub-contractors, implement an effective system of monitoring and reports analysing access to and use of the Supplier Information Management System, the Development Environment, the Government Data and the Code to:

(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

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

21.2 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 Government 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

21.3 The Supplier must ensure that, unless the Buyer 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 Buyer

21.4 The Supplier must provide the Buyer 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

21.5 The Buyer may at any time require the Supplier to update the Protective Monitoring System to:

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

(b) implement additional audit and monitoring requirements; and

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

22 Audit rights

Right of audit

22.1 The Buyer 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 16 (Security) and the Data Protection Laws as they apply to Government Data;

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

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

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

22.2 Any audit undertaken under this Paragraph 22:

(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 Buyer has under this Contract.

22.3 The Buyer may not undertake more than one audit under Paragraph 22.1 in each calendar year unless the Buyer 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 Government Data;

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

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

(i) an IT Health Check; or

(ii) a Breach of Security.

Conduct of audits

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

22.5 The Buyer 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 Buyer 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.

22.6 The Supplier must, and must ensure that Sub-contractors, on demand provide the Buyer with all co-operation and assistance the Buyer may reasonably require, including:

(a) all information requested by the Buyer 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

22.7 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 Government Data; or

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

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

22.8 The exercise by the Buyer 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.

23 Breach of Security

Reporting Breach of Security

23.1 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

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

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

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

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

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

Subsequent action

23.3 As soon as reasonably practicable and, in any event, within 5 Working Days, or such other period agreed with the Buyer, following the Breach of Security, provide to the Buyer:

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

(b) if required by the Buyer:

(i) a root cause analysis; and

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

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

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

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

(i) how the issue will be remedied;

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

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

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

(c) the Supplier's communication and engagement activities in respect of the Breach of Security, including any communication or engagement with individuals affected by any Breach of Security that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data;

(d) the infrastructure, services and systems (including any contact centre facilities) the Supplier will establish to undertake the remediation, communication and engagement activities.

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

23.6 The Buyer 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 10 Working Days of the date on which the Buyer rejected the draft Breach Action Plan submit a revised draft Breach Action Plan that takes into account the Buyer's reasons; and

(ii) Paragraph 23.5 and 23.6 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.

23.7 When implementing the Breach Action Plan, the Supplier must:

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

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

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

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

(e) continue to implement the Breach Action Plan until the Buyer indicates that the Breach of Security and the impacts on the Buyer, the Government Data, the Code and the affected individuals have been resolved to the Buyer's satisfaction.

23.8 The obligation to provide and implement a Breach Action Plan under Paragraphs 23.3 to 23.7 continues notwithstanding the expiry or termination of this Contract.

Costs of preparing and implementing a Breach Action Plan

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

Reporting of Breach of Security to regulator

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

(a) make that report within the time limits:

(i) specified by the relevant regulator; or

(ii) otherwise required by Law;

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

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

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

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

24 Return and Deletion of Government Data

24.1 The Supplier must create and maintain a register of:

(a) all Government Data the Supplier, or any Sub-contractor, receives from or creates for the Buyer; 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 Government Data is stored,

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

24.2 The Supplier must:

(a) review and update the Government Data Register:

(i) within 10 Working Days of the Supplier or any Sub-contractor changes those parts of the Supplier Information Management System on which the Government Data is stored;

(ii) within 10 Working Days of a significant change in the volume, nature or overall sensitivity of the Government Data stored on the Supplier Information Management System;

(iii) at least once every 12 (twelve) months; and

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

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

(ii) otherwise when the Buyer requests.

24.3 Subject to Paragraph 24.4, the Supplier must, and must ensure that all Subcontractors, securely erase any or all Government Data held by the Supplier or Subcontractor, including any or all Code:

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

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

24.4 Paragraph 24.4 does not apply to Government Data:

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

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

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

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

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

(b) using the method specified by the Buyer.

Annex 2 Security Management Plan Template

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

Annex 3 Sub-contractor Security Requirements

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

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

Annex 4 Secure by Design Questionnaire

[**To be used only where the Buyer has selected the relevant option in Paragraph 1**]

Secure by Design Principle	Requirements	How the Supplier will meet the requirement
Principle 1 Create responsibility for cyber security risk Assign a designated risk owner to be accountable for managing cyber security risks for the service within the contract. This must be a senior stakeholder with the experience, knowledge and authority to lead on security activities.	The Supplier designates a senior individual within their organisation who has overall accountability for ensuring the Secure by Design are met as part of the overall security requirements stated within the contract.	
	The Supplier designates a senior individual within the supplier delivery team - who will be reporting to the SRO, service owner or equivalent - with overall responsibility for the management of cyber security risks of digital services and technical infrastructure during their delivery.	
	The Supplier provides adequate and appropriately qualified resources to support the Buyer with following the government Secure by Design Approach as part of service delivery. These resources must be reviewed at the beginning of each of the delivery phases during the delivery lifecycle of the service as agreed with the Buyer.	
Principle 2	The Supplier carries out proportionate (risk-driven) security reviews of third-party products before they are considered as a component of the digital service. The type and details of the review should be based on the significance	

Secure by Design Principle	Requirements	How the Supplier will meet the requirement
Source secure technology products Where third-party products are used, perform security due diligence by continually assessing platforms, software and code for security vulnerabilities. Mitigate risks and share findings with suppliers to help them improve product security.	associated with the product and are subject to agreement with the Buyer.	
	The Supplier takes reasonable steps to reduce potential cyber security risks associated with using a third-party product as part of the service to a level that meets the Buyer's security risk appetite for the service. Where the risk cannot be mitigated to such level, the Buyer should be informed and asked to accept the risk associated with using the product.	
	The Supplier takes reasonable steps to assess third-party products used as a component of the digital service against legal and regulatory obligations and industry security standards specified by the Buyer. Where the product doesn't meet the required obligations, the Supplier must discuss with the Buyer the residual risks associated with using the product.	
Principle 3 Adopt a risk-driven approach Establish the project's risk appetite and maintain an assessment of cyber security risks to build protections appropriate to the evolving threat landscape.	As provided by the Buyer, the Supplier should share the risk appetite across the supplier's delivery team from the outset.	
	The Supplier supports the Buyer with identifying the cyber threats and attack paths as part of ongoing threat modelling during digital service delivery.	
	The Supplier supports the Buyer with assessing cyber security risks and providing risk analysis details to help risk owners make informed risk decisions.	

Secure by Design Principle	Requirements	How the Supplier will meet the requirement
	During the assessment, risks to the digital service are identified, analysed, prioritised, and appropriate mitigation is proposed taking into account the risk appetite during the lifecycle of the service.	
	The Supplier produces an output from the risk management process containing a clear set of security requirements that will reduce the risks in line with the agreed risk appetite and cyber security risk management approach.	
	The Supplier factors in the legal and regulatory requirements provided by the Buyer in the risk management process and service design and build.	
Principle 4 Design usable security controls Perform regular user research and implement findings into service design to make sure security processes are fit for purpose and easy to understand.	The Supplier ensures that security requirements that are defined and documented as part of user research activities (for example user stories and user journeys) are fed into the design of the digital service.	
	The Supplier ensures that business objectives informing security requirements listed in the business case for the digital service are taken into consideration when designing security controls.	
Principle 5 Build in detect and respond security	The Supplier responsible for building the digital service ensures that proportionate security logging, monitoring and alerting mechanisms able to discover cyber security events and vulnerabilities documented in the threat and risk assessment are designed into the service.	

Secure by Design Principle	Requirements	How the Supplier will meet the requirement
Design for the inevitability of security vulnerabilities and incidents. Integrate appropriate security logging, monitoring, alerting and response capabilities. These must be continually tested and iterated.	The Supplier responsible for building the digital service integrates incident response and recovery capabilities that are in line with the requirements and timescales documented in the service resilience or similar documentation.	
	The Supplier responsible for building the digital service regularly tests digital services and infrastructure to identify and fix weaknesses within systems.	
Principle 6 Design flexible architectures Implement digital services and update legacy components to allow for easier integration of new security controls in response to changes in business requirements, cyber threats and vulnerabilities.	As agreed with the Buyer, the Supplier responsible for building the digital service uses flexible architectures and components that allow integration of new security measures in response to changes in business requirements, cyber threats and vulnerabilities.	
	The Supplier responsible for building the digital service tests security controls and verifying they are fit for purpose before deployment.	
Principle 7 Minimise the attack surface Use only the capabilities, software, data and hardware components necessary for a service to mitigate cyber security	The Supplier responsible for building the digital service implements risk-driven security controls which meet the risk appetite and appropriate baseline as agreed with the Buyer.	
	The Supplier responsible for building the digital service follows secure coding practices and, with consultation with the Buyer's delivery team, identifies and mitigates	

Secure by Design Principle	Requirements	How the Supplier will meet the requirement
risks while achieving its intended use.	vulnerabilities proactively reducing the number of vulnerabilities that potential attackers can exploit.	
	The Supplier retires service components (including data) securely when they are no longer needed, or at the end of their lifecycle.	
Principle 8 Defend in depth Create layered controls across a service so it's harder for attackers to fully compromise the system if a single control fails or is overcome.	The Supplier responsible for building the digital service adopts a defence in depth approach when designing the security architecture for the digital service.	
	The Supplier responsible for building the digital service implements security measures to incorporate segmentation.	
	The Supplier responsible for building the digital service implements mechanisms to keep the impact of potential security incidents contained.	
	The Supplier responsible for building the digital service tests security controls and verifying they are fit for purpose before deployment.	
Principle 9 Embed continuous assurance	The Supplier responsible for building the digital service reassess controls during build to ensure they operate effectively and that no known vulnerabilities exist.	

Secure by Design Principle	Requirements	How the Supplier will meet the requirement
Implement continuous security assurance processes to create confidence in the effectiveness of security controls, both at the point of delivery and throughout the operational life of the service.	The Supplier responsible for building the digital service reassesses security controls against changes in the service or threat landscape during the build phase.	
	The Supplier responsible for building the digital service reports on how the delivery team follows the Secure by Design Approach and adheres to the Secure by Design principles by contributing to the maintenance of the Secure by Design Self Assessment Tracker.	
Principle 10 Make changes securely Embed security into the design, development and deployment processes to ensure that the security impact of changes is considered alongside other factors.	The Supplier responsible for building the digital service works with the Buyer to assess the security impact of changes before these are made to digital services and infrastructure.	
	The Supplier responsible for building the digital service records any residual unmitigated risks to the cyber security risk register and shares this with the accountable individuals and security function responsible for incorporating these into the organisation's risk registers.	