# Call-Off Schedule 9 (Security)

# Short Form Security Schedule

## 1 Supplier obligations

**Core requirements**

1.1 The Supplier must comply with the core requirements set out in Paragraphs 4 to 9.

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

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

| |
|---|
| |

**Optional requirements**

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

| | |
|---|---|
| **Security Management Plan** (see Paragraph 1) | |
| The Supplier must provide the Buyer with a Security Management Plan detailing how the requirements for the options selected in this table have been met. | ☒ |
| **Buyer Security Policies** (see Paragraph 11) | |
| The Buyer requires the Supplier to comply with the following policies relating to security management:<br>The following Buyer security policy, which the Buyer may change from time to time:<br>  <br>Information Security Policy.pdf<br>The Buyer shall notify the Supplier in writing of any updates to the security policy which the Supplier is required to comply with.<br>• | ☒ |
| **Security testing** (see Paragraph 12) | |
| The Supplier must undertake security testing at least once every Contract Year and remediate any vulnerabilities, where it is technically feasible to do so | ☒ |
| **Cloud Security Principles** (see Paragraph 13) | |
| The Supplier must ensure that the Cloud Providers assess the Cloud Services against the Cloud Security Principles | ☒ |
| **Record keeping** (see Paragraph 14) | |
| The Supplier must keep records relating to Subcontractors, Sites, Third-party Tools and third parties | ☒ |
| **Encryption** (see Paragraph 15) | |
| The Supplier must encrypt Government Data while at rest or in transit | ☒ |
| **Protective Monitoring System** (see Paragraph 16) | |
| The Supplier must implement an effective Protective Monitoring System | ☒ |
| **Patching** (see Paragraph 17) | |
| The Supplier must patch vulnerabilities in the Supplier System promptly | ☒ |
| **Malware protection** (see Paragraph 18) | |

| | |
|---|---|
| The Supplier must use appropriate Anti-virus Software | ☒ |
| **End-user Devices** (see Paragraph 19) | |
| The Supplier must manage End-user Devices appropriately | ☒ |
| **Vulnerability scanning** (see Paragraph 20) | |
| The Supplier must scan the Supplier System monthly for unpatched vulnerabilities | ☒ |
| **Access control** (see Paragraph 21) | |
| The Supplier must implement effective access control measures for those accessing Government Data and for Privileged Users | ☒ |
| **Remote Working** (see Paragraph 22) | |
| The Supplier may allow Supplier Staff to undertake Remote Working once an approved Remote Working Policy is in place | ☒ |
| **Backup and recovery of Government Data** (see Paragraph 23) | |
| The Supplier must have in place systems for the backup and recovery of Government Data | ☒ |
| **Return and deletion of Government Data** (see Paragraph 24) | |
| The Supplier must return or delete Government Data when requested by the Buyer | ☒ |
| **Physical security** (see Paragraph 25) | |
| The Supplier must store Government Data in physically secure locations | ☒ |
| **Security breaches** (see Paragraph 26) | |
| The Supplier must report any Breach of Security to the Buyer promptly | ☒ |

## 2 Definitions

**"Anti-virus Software"** means software that:

(a) protects the Supplier System from the possible introduction of Malicious Software;

(b) scans for and identifies possible Malicious Software in the Supplier System;

(c) if Malicious Software is detected in the Supplier System, so far as possible:

(i) prevents the harmful effects of the Malicious Software; and

(ii) removes the Malicious Software from the Supplier System;

| | |
|---|---|
| **"BPSS"** | 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; |
| **"Breach of Security"** | means the occurrence of:<br>(a) any unauthorised access to or use of the Services, the Sites, the Supplier System and/or the Government Data;<br>(b) the loss (physical or otherwise), corruption and/or unauthorised disclosure of any Government Data, including copies of such Government Data; and/or<br>(c) any part of the Supplier System ceasing to be compliant with the required Certifications;<br>(d) the installation of Malicious Software in the Supplier System:<br>(e) any loss of operational efficiency or failure to operate to specification as the result of the installation or operation of Malicious Software in the Supplier System; and<br>(f) includes any attempt to undertake the activities listed in sub-Paragraph (a) where the Supplier has reasonable grounds to suspect that attempt:<br>(i) was part of a wider effort to access information and communications technology operated by or on behalf of Central Government Bodies; or<br>(ii) was undertaken, or directed by, a state other than the United Kingdom; |
| **"Buyer Equipment"** | means any hardware, computer or telecoms devices, and equipment that forms part of the Buyer System; |
| **"Buyer Security Policies"** | means those securities specified by the Buyer in Paragraph 1.3; |
| **"Certifications"** | means one or more of the following certifications (or equivalent):<br>(a) ISO/IEC 27001:2022 by a UKAS-recognised Certification Body in respect of the Supplier System, or in respect of a wider system of which the Supplier System forms part; and<br>(a) Cyber Essentials Plus; and/or<br>(b) Cyber Essentials; |
| **"CHECK Scheme"** | means the NCSC's scheme under which approved companies can conduct authorised penetration tests of public sector and critical national infrastructure systems and networks; |

| | |
|---|---|
| **"CHECK Service Provider"** | means a company which, under the CHECK Scheme:<br>(a) has been certified by the NCSC;<br>(b) holds "Green Light" status; and<br>(c) is authorised to provide the IT Health Check services required by Paragraph 7 (*Security Testing*); |
| **"Cloud Security Principles"** | means the NCSC's document "Implementing the Cloud Security Principles" as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles; |
| **"CREST Service Provider"** | means a company with an information security accreditation of a security operations centre qualification from CREST International; |
| **"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 NCSC; |
| **"Developed System"** | means the software or system that the Supplier is required to develop under this Contract; |
| **"End-user Device"** | means any personal computers, laptops, tablets, terminals, smartphones or other portable electronic devices used in the provision of the Services; |
| **"Expected Behaviours"** | means the expected behaviours set out and updated from time to time in the Government Security Classification Policy, currently found at paragraphs 12 to 16 and in the table below paragraph 16 of https://www.gov.uk/government/publications/government-security-classifications/guidance-11-working-at-official-html; |
| **"Government Security Classification Policy"** | means the policy, as updated from time to time, establishing an administrative system to protect information assets appropriately against prevalent threats, including classification tiers, protective security controls and baseline behaviours, the current version of which is found at https://www.gov.uk/government/publications/government-security-classifications; |
| **"Handle"** | means any operation performed on data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of that data; |
| **"IT Health Check"** | means the security testing of the Supplier System; |
| **"Malicious Software"** | has the meaning given in Call-Off Schedule 6 (ICT Services); |

| | |
|---|---|
| **"NCSC"** | means the National Cyber Security Centre, or any successor body performing the functions of the National Cyber Security Centre; |
| **"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; |
| **"Privileged User"** | means a user with system administration access to the Supplier System, or substantially similar access privileges; |
| **"Prohibition Notice"** | means the meaning given to that term by Paragraph 5.4. |
| **"Protective Monitoring System"** | has the meaning given to that term by Paragraph 16.1; |
| **"Relevant Conviction"** | 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; |
| **"Remote Location"** | means a location other than a Supplier's or a Subcontractor'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 Subcontractor's Site; |
| **"Remote Working Policy"** | the policy prepared and approved under Paragraph 22 under which Supplier Staff are permitted to undertake Remote Working; |
| **"Security Controls"** | means the security controls set out and updated from time to time in the Government Security Classification Policy, currently found at Paragraph 12 of https://www.gov.uk/government/publications/government-security-classifications/guidance-15-considerations-for-security-advisors-html; |
| **"Staff Vetting Procedure"** | means the procedure for vetting Supplier Staff set out in Paragraph 6; |
| **"Subcontractor Staff"** | means:<br>(a) any individual engaged, directly or indirectly, or employed, by any Subcontractor; and<br>(b) engaged in or likely to be engaged in:<br>(i) the performance or management of the Services; or<br>(ii) the provision of facilities or services that are necessary for the provision of the Services; |
| **"Supplier System"** | has the meaning given in Call-Off Schedule 6 (ICT Services); |
| **"Third-party Tool"** | means any software used by the Supplier by which the Government Data is accessed, analysed or modified, or some form of operation is performed on it; |

| | |
|---|---|
| **"UKAS-recognised Certification Body"** | means:<br>(a) an organisation accredited by UKAS to provide certification of ISO/IEC27001:2013 and/or ISO/IEC27001:2022; or<br>(b) an organisation accredited to provide certification of ISO/IEC27001:2013 and/or ISO/IEC27001:2022 by a body with the equivalent functions as UKAS in a state with which the UK has a mutual recognition agreement recognising the technical equivalence of accredited conformity assessment. |

## Part One: Core Requirements

## 3 Handling Government Data

3.1 The Supplier acknowledges that it:

(a) must only Handle Government Data that is classified as OFFICIAL; and

(b) must not Handle Government Data that is classified as SECRET of TOP SECRET.

3.2 The Supplier must:

(a) not alter the classification of any Government Data

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

(i) immediately inform the Buyer; and

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

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

(a) the Expected Behaviours; and

(b) the Security Controls.

## 4 Certification Requirements

4.1 Where the Buyer has not specified Certifications under Paragraph 1, the Supplier must ensure that it and any Subcontractors that Handle Government Data are certified as compliant with Cyber Essentials (or equivalent).

4.2 Where the Buyer has specified Certifications under Paragraph 1, the Supplier must ensure that both:

(a) it; and

(b) any Subcontractor that Handles Government Data,

are certified as compliant with the Certifications specified by the Buyer in Paragraph 1 (or equivalent certifications).

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

(a) before the Supplier or any Subcontractor Handles Government Data; and

(b) throughout the Term.

## 5 Location

5.1 Where the Buyer has not specified any locations or territories in Paragraph 1, the Supplier must not, and ensure that Subcontractors do not store, access or Handle Government Data outside:

(a) the United Kingdom; or

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

5.2 Where the Buyer has specified locations or territories in Paragraph 1, the Supplier must, and ensure that all Subcontractors, at all times store, access or Handle Government Data only in or from the geographic areas specified by the Buyer.

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

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

(b) that binding agreement includes obligations on the entity in relation to security management at least as onerous as those relating to Subcontractors in this Call-Off Schedule 9 (Security);

(c) the Supplier or Subcontractor has taken reasonable steps to assure itself that:

(i) the entity complies with the binding agreement; and

(ii) the Subcontractor's system has in place appropriate technical and organisational measures to ensure that the Subcontractor will store, access, manage and/or Handle the Government Data as required by this Call-Off Schedule 9 (Security);

(d) the Buyer has not given the Supplier a Prohibition Notice under Paragraph 5.4.

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

5.5 Where the Supplier has received a Prohibition Notice, the Supplier must, and must ensure its Subcontractors, comply with the requirements of the Prohibition Notice within 40 Working Days of the date of the notice.

## 6 Staff vetting

6.1 The Supplier must not allow Supplier Staff, and must ensure that Subcontractors do not allow Subcontractor Staff, to access or Handle Government Data, if that person:

(a) has not completed the Staff Vetting Procedure; or

(b) where no Staff Vetting Procedure is specified in the Order Form:

(i) has not undergone the checks required for the BPSS to verify:

(A) the individual's identity;

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

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

(D) that the individual has no Relevant Convictions; and

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

6.2 Where the Supplier considers it cannot ensure that a Subcontractor will undertake the relevant security checks on any Subcontractor 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 Subcontractor, its vetting processes and the roles the affected Subcontractor 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 Subcontractor Staff and the management of the Subcontractor.

## 7 Supplier assurance letter

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

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

(b) it has fully complied with all requirements of this Call-Off Schedule 9 (Security); and

(c) all Subcontractors have complied with the requirements of this Call-Off Schedule 9 (Security) with which the Supplier is required to ensure they comply;

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

## 8 Assurance

8.1 The Supplier must provide such information and documents as the Buyer may request in order to demonstrate the Supplier's and any Subcontractors' compliance with this Call-Off Schedule 9 (Security).

8.2 The Supplier must provide that information and those documents:

(a) at no cost to the Buyer;

(b) within 10 Working Days of a request by the Buyer;

(c) except in the case of an original document, in the format and with the content and information required by the Buyer; and

(d) in the case of an original document, as a full, unedited and unredacted copy.

## 9 Use of Subcontractors and third parties

9.1 The Supplier must ensure that Subcontractors and any other third parties that store, have access to or Handle Government Data comply with the requirements of this Call-Off Schedule 9 (Security).

## Part Two: Additional Requirements

## 10 Security Management Plan

10.1 This Paragraph 10 applies only where the Buyer has selected this option in Paragraph 1.3.

**Preparation of Security Management Plan**

10.2 The Supplier shall document in the Security Management Plan how the Supplier and its Subcontractors shall comply with the requirements set out in this Call-Off Schedule 9 (Security) and the Contract in order to ensure the security of the Supplier solution and the Buyer Data.

10.3 The Supplier shall prepare and submit to the Buyer within 20 Working Days of the Start Date of this Contract, the Security Management Plan, which must include a description of how all the options selected in this schedule are being met along with evidence of the required certifications for the Supplier and any Subcontractors specified in Paragraph 4.

**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 operate the service and process Buyer 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 10.5 shall be repeated until such time as the Buyer issues a information security approval statement to the Supplier or terminates this Contract.

10.7 The rejection by the Buyer of a second revised Security Management 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 updated version 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 System;

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

(c) a vulnerability to the components or architecture of the Supplier 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 indicates significant concerns.

10.10 Within 10 Working Days of notifying the Buyer in accordance with paragraph 10.9 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 Buyer Security Policies

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

11.2 If there is an inconsistency between the Buyer Security Policies and the requirement of this Call-Off Schedule 9 (Security), then the requirements of this Schedule will prevail to the extent of that inconsistency.

## 12 Security testing

12.1 The Supplier must:

(a) before Handling Government Data; and

(b) at least once during each Contract Year,

undertake the following activities:

(c) conduct security testing of the Supplier System (an "**IT Health Check**") in accordance with Paragraph 12.2; and

(d) implement any findings, and remedy any vulnerabilities identified by the IT Health Check in accordance with Paragraph 12.3.

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

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

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

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

(d) ensure that the IT Health Check provides for effective penetration testing of the Supplier System.

12.3 The Supplier shall treat any vulnerabilities as follows:

(a) the Supplier must remedy any vulnerabilities classified as high in the IT Health Check report:

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

(ii) if it is technically feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 12.3(a)(i), then as soon as reasonably practicable after becoming aware of the vulnerability and its classification;

(b) the Supplier must remedy any vulnerabilities classified as high in the IT Health Check report:

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

(ii) if it is technically feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 12.3(b)(i), then as soon as reasonably practicable after becoming aware of the vulnerability and its classification;

(c) the Supplier must remedy any vulnerabilities classified as medium in the IT Heath Check report:

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

(ii) if it is technically feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 12.3(c)(i), then as soon as reasonably practicable after becoming aware of the vulnerability and its classification;

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

## 13 Cloud Security Principles

13.1 The Supplier must ensure that the Cloud Providers comply with the Cloud Security Principles.

13.2 The Supplier must ensure that the Cloud Providers assess the Cloud Services (as applicable to the relevant Cloud Provider) against the Cloud Security Principles to assure the Supplier that each Cloud Provider complies with Paragraph 13.1:

(a) before Handling Government Data;

(b) at least once each Contract Year; and

(c) when required by the Buyer.

13.3 Where the Cloud Security Principles provide for various options, each Cloud Provider must document the option it has chosen to implement and its reasons for doing so.

13.4 The Supplier must:

(a) keep records of any assessment made under Paragraph 13.2; and

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

## 14 Information about Subcontractors, Sites and Third-party Tools

14.1 The Supplier must keep the following records:

(a) for Subcontractors or third parties that store, have access to or Handle Government Data:

(i) the Subcontractor or third-party's:

(A) legal name;

(B) trading name (if any); and

(C) registration details (where the Subcontractor is not an individual), including:

(1) country of registration;

(2) registration number (if applicable); and

(3) registered address;

(ii) the Certifications held by the Subcontractor or third party;

(iii) the Sites used by the Subcontractor or third party;

(iv) the Services provided or activities undertaken by the Subcontractor or third party;

(v) the access the Subcontractor or third party has to the Supplier System;

(vi) the Government Data Handled by the Subcontractor or third party; and

(vii) the measures the Subcontractor or third party has in place to comply with the requirements of this Call-Off Schedule 9 (Security);

(b) for Sites from or at which Government Data is accessed or Handled:

(i) the location of the Site;

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

(A) legal name;

(B) trading name (if any); and

(C) registration details (where the Subcontractor is not an individual);

(iii) the Certifications that apply to the Site;

(iv) the Government Data stored at, or Handled from, the site; and

(c) for Third-party Tools:

(i) the name of the Third-party Tool;

(ii) the nature of the activity or operation performed by the Third-party Tool on the Government Data; and

(iii) in respect of the entity providing the Third-party Tool, its:

(A) full legal name;

(B) trading name (if any)

(C) country of registration;

(D) registration number (if applicable); and

(E) registered address.

14.2 The Supplier must update the records it keeps in accordance with Paragraph 14.1:

(a) at least four times each Contract Year;

(b) whenever a Subcontractor, third party that accesses or Handles Government Data, Third-party Tool or Site changes; or

(c) whenever required to go so by the Buyer.

14.3 The Supplier must provide copies of the records it keeps in accordance with Paragraph 14.1 to the Buyer within 10 Working Days of any request by the Buyer.

## 15 Encryption

15.1 The Supplier must, and must ensure that all Subcontractors, encrypt Government Data:

(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.

## 16 Protective Monitoring System

16.1 The Supplier must, and must ensure that Subcontractors, implement an effective system of monitoring and reports, analysing access to and use of the Supplier System and the Government Data to:

(a) identify and prevent any potential Breach of Security;

(b) respond effectively and in a timely manner to any Breach of Security;

(c) identify and implement changes to the Supplier System to prevent any future Breach of Security; and

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

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

16.2 The Protective Monitoring System must provide for:

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

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

## 17 Patching

17.1 The Supplier must, and must ensure that Subcontractors, treat any public releases of patches for vulnerabilities as follows:

(a) the Supplier must patch any vulnerabilities classified as "critical":

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

(ii) if it is technically feasible to patch the vulnerability but not technically feasible to do so as required by Paragraph 17.1(a)(i), then as soon as reasonably practicable after the public release;

(b) the Supplier must patch any vulnerabilities classified as "important":

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

(ii) if it is technically feasible to patch the vulnerability but not technically feasible to do so as required by Paragraph 17.1(b)(i), then as soon as reasonably practicable after the public release;

(c) the Supplier must remedy any vulnerabilities classified as "other" in the public release:

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

(ii) if it is technically feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 17.1(c)(i), then as soon as reasonably practicable after the public release;

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

## 18 Malware protection

18.1 In accordance with paragraph 9.7 of Call-Off Schedule 6 (ICT Services), the Supplier shall install and maintain Anti-virus Software or procure that Anti-virus Software is installed and maintained on the Supplier System.

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

(a) prevents the installation of the most common forms of Malicious Software in the Supplier System;

(b) performs regular scans of the Supplier System to check for Malicious Software; and

(c) where Malicious Software has been introduced into the Supplier System, so far as practicable:

(i) prevents the harmful effects from the Malicious Software; and

(ii) removes the Malicious Software from the Supplier System.

## 19 End-user Devices

19.1 The Supplier must, and must ensure that all Subcontractors, manage all End-user Devices on which Government Data is stored or Handled in accordance with the following requirements:

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

(b) users must authenticate before gaining access;

(c) all Government Data must be encrypted using a suitable encryption tool;

(d) the End-user Device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the End-user Device is inactive;

(e) the End-User Device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Government Data to ensure the security of that Government Data;

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

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

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

## 20 Vulnerability scanning

20.1 The Supplier must:

(a) scan the Supplier System 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 17.

## 21 Access control

21.1 The Supplier must, and must ensure that all Subcontractors:

(a) identify and authenticate all persons who access the Supplier System 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 System and Sites that those persons require;

(d) maintain records detailing each person's access to the Supplier System.

21.2 The Supplier must ensure, and must ensure that all Subcontractors ensure, that the user accounts for Privileged Users of the Supplier 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 System after a period of time that is proportionate to the risk environment during which the account is inactive; and

(f) are:

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

(ii) time limited; and

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

## 22 Remote Working

22.1 The Supplier must ensure, and ensure that Subcontractors ensure, that:

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

(b) where the Buyer permits Remote Working by Privileged Users, such Remote Working takes place only in accordance with any conditions imposed by the Buyer.

22.2 Where the Supplier or a Subcontractor 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 Subcontractors 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) not permit any Supplier Staff or any Subcontractor to undertake Remote Working until the Remote Working Policy is approved by the Buyer.

22.3 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 Subcontractor (as appropriate); and

(ii) complies with the requirements set out in Paragraph 19 (*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); and

(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 Subcontractor (as applicable) will implement to mitigate the identified risks; and

(iv) the business rules with which the Supplier Staff must comply.

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

## 23 Backup and recovery of Government Data

23.1 The Supplier must ensure that the Supplier System:

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

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

23.2 The Supplier must ensure the Supplier System:

(a) uses backup locations for Government Data that are physically and logically separate from the rest of the Supplier System;

(b) 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;

(c) any backup failure is remedied promptly;

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

(i) identify any recovery failure; and

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

(e) any recovery failure is promptly remedied.

## 24 Return and deletion of Government Data

24.1 Subject to Paragraph 24.2, when requested to do so by the Buyer, the Supplier must, and must ensure that all Subcontractors:

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

(b) provide the Buyer with copies of any or all Government Data held by the Supplier or Subcontractor using the method specified by the Buyer.

24.2 Paragraph 24.1 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.

24.3 The Supplier must, and must ensure that all Subcontractors, provide the Buyer with copies of any or all Buyer Data held by the Supplier or Subcontractor:

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

(b) using the method specified by the Buyer.

## 25 Physical security

25.1 The Supplier must, and must ensure that Subcontractors, store the Government Data on servers housed in physically secure locations.

## 26 Breach of Security

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

(a) notify the Buyer as soon as reasonably practicable after becoming aware of the breach, and in any event within 24 hours;

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

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

(d) where the Breach of Security results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data, undertake any communication or engagement activities required by the Buyer with the individuals affected by the Breach of Security.