# Call-Off Schedule 9B (Security: Consultancy)

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

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

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

## 1. Buyer Options

### Risk assessment

| | | |
|---|---|---|
| The Buyer has assessed the Contract as:<br>***[Buyer Guidance: Include an "X" against the applicable item in the final column opposite]*** | a standard consultancy agreement | ☐ |
| | a higher-risk consultancy agreement | ☐ |

### Relevant Certifications

| | | |
|---|---|---|
| Where the Buyer has assessed the Contract as a standard consultancy agreement, it requires the Supplier to be certified as compliant with: | No certification required | ☐ |
| | Cyber Essentials (or equivalent) | ☐ |
| | Cyber Essentials Plus (or equivalent) | ☐ |

### Buyer Security Policies

| | |
|---|---|
| The Buyer requires the Supplier to comply with the following policies relating to security management:<br>• ***[Buyer Guidance: List Buyer security policies with which the Supplier and Sub-contractors must comply]*** | ☐ |

### Staff vetting

| | |
|---|---|
| The Buyer requires a staff vetting procedure other than BPSS. Where the Buyer selects this option, the alternative staff vetting procedure with which the Supplier must comply is:<br>• ***[Buyer Guidance: Set out any Buyer staff vetting procedure with which the Supplier and Sub-contractors must comply]*** | ☐ |

## 2. Supplier obligations

2.1 Where the Buyer has assessed the Contract as a higher-risk consultancy agreement, the Supplier must comply with all requirements in this Schedule.

2.2 Where the Buyer has assessed the Contract as a standard consultancy agreement, the Supplier must comply with this Schedule, other than:

2.2.1 the requirement to be certified as compliant with ISO/IEC 27001:2022 (or equivalent) under Paragraph 7.1.2;

2.2.2 the requirement to undertake security testing of the Supplier Information Management System in accordance with Paragraph 9 of Appendix 1; and

2.2.3 the requirement to produce a Security Management Plan in accordance with Paragraph 9.

## 3. Definitions

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

**"Anti-virus Software"** 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;

**"Breach of Security"** the occurrence of:

(a) any unauthorised access to or use of the Services, the Sites, the Supplier System and/or the Government Data;

(b) the loss (physical or otherwise), corruption and/or unauthorised disclosure of any Government Data, including copies of such Government Data; and/or

(c) any part of the Supplier System ceasing to be compliant with the Relevant Certifications;

(d) the installation of Malicious Software in the Supplier 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 Supplier System; and

(f) includes any attempt to undertake the activities listed in sub-Paragraph (a) where the Supplier has reasonable grounds to suspect that attempt:

(i) was part of a wider effort to access information and communications technology operated by or on behalf of Central Government Bodies; or

(ii) was undertaken, or directed by, a state other than the United Kingdom;

**"Certification Default"** the occurrence of one or more of the circumstances listed in Paragraph 7.4;

**"Certification Rectification Plan"** the plan referred to in Paragraph 7.5.1;

| | |
|---|---|
| **"Certification Requirements"** | the information security requirements set out in Paragraph 7; |
| **"CHECK Scheme"** | the NCSC's scheme under which approved companies can conduct authorised penetration tests of public sector and critical national infrastructure systems and networks; |
| **"CHECK Service Provider"** | a company which, under the CHECK Scheme:<br>(a) has been certified by the National Cyber Security Centre;<br>(b) holds "Green Light" status; and<br>(c) is authorised to provide the IT Health Check services required by Paragraph 9 of Appendix 1; |
| **"CHECK Team Leader"** | an individual with a CHECK Scheme team leader qualification issued by the NCSC; |
| **"CHECK Team Member"** | an individual with a CHECK Scheme team member qualification issued by the NCSC; |
| **"Cyber Essentials"** | the Cyber Essentials certificate issued under the Cyber Essentials Scheme; |
| **"Cyber Essentials Plus"** | the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme; |
| **"Cyber Essentials Scheme"** | the Cyber Essentials scheme operated by the National Cyber Security Centre; |
| **"End-user Device"** | any personal computers, laptops, tablets, terminals, smartphones or other portable electronic device provided by the Supplier or a Sub-contractor and used in the provision of the Services; |

| | |
|---|---|
| **"Expected Behaviours"** | the expected behaviours set out and updated from time to time in the Government Security Classification Policy, currently found at paragraphs 12 to 16 and in the table below paragraph 16 of https://www.gov.uk/government/publications/government-security-classifications/guidance-11-working-at-official-html; |
| **"Government Security Classification Policy"** | the policy, as updated from time to time, establishing an administrative system to protect information assets appropriately against prevalent threats, including classification tiers, protective security controls and baseline behaviours, the current version of which is found at https://www.gov.uk/government/publications/government-security-classifications; |
| **"HMG Baseline Personnel Security Standard"** | the employment controls applied to any individual member of the Supplier Staff that performs any activity relating to the provision or management of the Services, as set out in "HMG Baseline Personnel Standard", Version 7.0, June 2024(https://www.gov.uk/government/publications/government-baseline-personnel-security-standard ), as that document is updated from time to time; |
| **"NCSC Device Guidance"** | the National Cyber Security Centre'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"** | a user with system administration access to the Supplier Information Management System, or substantially similar access privileges; |
| **"Prohibited Activity"** | the storage, access or Handling of Government Data prohibited by a Prohibition Notice; |
| **"Prohibition Notice"** | a notice issued under Paragraph 1.2 of Appendix 1; |
| **"Relevant Certifications"** | those certifications specified in Paragraph 7.1; |
| **"Relevant Convictions"** | any previous or pending prosecution, conviction or caution (excluding any spent conviction under the Rehabilitation of Offenders Act 1974) relating to offences involving dishonesty, terrorism, immigration, |

| | |
|---|---|
| | firearms, fraud, forgery, tax evasion, offences against people (including sexual offences), or any other offences relevant to Services as the Buyer may specify; |
| **"Remote Location"** | a location other than a Supplier's or a Sub-contractor's Site; |
| **"Remote Working"** | the provision or management of the Services by Supplier Staff from a location other than a Supplier's or a Sub-contractor's Site; |
| **"Remote Working Policy"** | the policy prepared and approved under Paragraph 3.9 of Appendix 1 under which Supplier Staff are permitted to undertake Remote Working; |
| **"Security Controls"** | the security controls set out and updated from time to time in the Government Security Classification Policy, currently found at Paragraph 12 of https://www.gov.uk/government/publications/government-security-classifications/guidance-15-considerations-for-security-advisors-html; |
| **"Security Management Plan"** | the document prepared in accordance with the requirements of Paragraph 9; |
| **"Standard Contractual Clauses"** | the standard data protection clauses specified in Article 46 of the United Kingdom General Data Protection Regulation setting out the appropriate safeguards for the transmission of personal data outside the combined territories of the United Kingdom and the European Economic Area; |
| **"Supplier Information Management System"** | (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; and<br>(b) the associated information assets and systems (including organisational structure, controls, policies, practices, procedures, processes and resources); |
| **"Sub-contractor"** | for the purposes of this Schedule only, any individual or entity that:<br>(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 and the Government Data,<br><br>and this definition shall apply to this Schedule in place of the definition of Sub-contractor in Joint Schedule 1 *(Definitions)*; |
| **"Supplier Staff"** | for the purposes of this Schedule only, any individual engaged, directly or indirectly, or employed by the Supplier or any Sub-contractor (as that term is defined for the purposes of this Schedule) in the management or performance of the Supplier's obligations under the Contract, and this definition shall apply to this Schedule in place of the definition of Supplier Staff in Joint Schedule 1 *(Definitions)*; |
| **"UKAS"** | the United Kingdom Accreditation Service; and |
| **UKAS-recognised Certification Body** | (a) an organisation accredited by UKAS to provide certification of ISO/IEC27001:2013 and/or ISO/IEC27001:2022; or<br><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. |

## 4. Introduction

4.1 This Schedule sets out:

4.1.1 the arrangements the Supplier must implement before, and comply with when, providing the Services and performing its other obligations under the Contract to ensure the security of the Government Data, the Services and the Supplier Information Management System;

4.1.2 the assessment of the Contract as either a:

(a) standard consultancy agreement; or

(b) higher-risk consultancy agreement,

in Paragraph 1;

4.1.3 the Buyer's access to the Supplier Staff and Supplier Information Management System, in Paragraph 6;

4.1.4 the Certification Requirements, in Paragraph 7;

4.1.5 in the case of higher-risk consultancy agreements, the requirements for a Security Management Plan in Paragraph 9; and

4.1.6 the security requirements with which the Supplier and Sub-contractors must comply in Appendix 1.

## 5. Principles of security

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

5.1.1 the Sites;

5.1.2 the Services; and

5.1.3 the Supplier's Information Management System.

5.2 The Supplier is responsible for:

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

5.2.2 the security of the Supplier Information Management System.

5.3 The Supplier must:

5.3.1 comply with the security requirements in Appendix 1; and

5.3.2 ensure that each Sub-contractor that Handles Government Data complies with the security requirements in Appendix 1.

5.4 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.

## 6. Access to Supplier Staff and Supplier Information Management System

6.1 The Buyer may require, and the Supplier must provide the Buyer and its authorised representatives with:

6.1.1 access to the Supplier Staff;

6.1.2 access to the Supplier Information Management System to audit the Supplier and its Sub-contractors' compliance with the Contract; and

6.1.3 such other information and/or documentation that the Buyer or its authorised representatives may reasonably require,

to assist the Buyer to establish whether the arrangements which the Supplier and its Sub-contractors have implemented in order to ensure

6.1.4 the security of the Government Data; and

6.1.5 the Supplier Information Management System are consistent with the representations in the Security Management Plan.

6.2 The Supplier must provide the access required by the Buyer in accordance with Paragraph 6.1 within [ten] Working Days of receipt of such request, except in the case of a Breach of Security in which case the Supplier shall provide the Buyer with the access that it requires within [24 hours] of receipt of such request.

## 7. Certification Requirements

7.1 The Supplier shall ensure that, unless otherwise agreed by the Buyer, it is certified as compliant with:

7.1.1 in the case of a standard consultancy agreement the option chosen by the Buyer in Paragraph 1; or

7.1.2 in the case of a higher-risk consultancy agreement:

(a) either:

(i) an ISO/IEC 27001:2022 certification by a UKAS-Recognised Certification Body in respect of the Supplier Information Management System (or an equivalent certification); or

(ii) where the Supplier Information Management System is included within the scope of a wider ISO/IEC 27001:2022 certification (or an equivalent certification) that certification; and

(b) Cyber Essentials Plus (or an equivalent certification) ("**Relevant Certifications"**).

7.2 Unless otherwise agreed by the Buyer, the Supplier must provide the Buyer with a copy of the Relevant Certifications before it begins to provide the Services.

7.3 The Supplier must ensure that at the time it begins to provide the Services, the Relevant Certifications are:

7.3.1 currently in effect;

7.3.2 together, relate to the full scope of the Supplier Information System; and

7.3.3 are not subject to any condition that may impact the provision of the Services.

7.4 The Supplier must notify the Buyer promptly, any in any event within three Working Days of becoming aware that:

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

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

7.4.3 the Relevant Certifications, together, no longer apply to the full scope of the Supplier Information Management System; and/or

7.4.4 the body that awarded a Relevant Certification has made it subject to conditions, the compliance with which may impact the provision of the Services (each a "**Certification Default**").

7.5 Where the Supplier has notified the Buyer of a Certification Default under Paragraph 7.4:

7.5.1 the Supplier must, within ten working Days of the date in which the Supplier provided notice under Paragraph 7.4 (or such other period as the Parties may agree) provide a draft plan (a "**Certification Rectification Plan**") to the Supplier setting out:

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

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

(c) the steps the Supplier will take to remedy the Certification Default;

7.5.2 the Buyer must notify the Supplier as soon as reasonably practicable whether it accepts or rejects the Certification Rectification Plan;

7.5.3 if the Buyer rejects the Certification Rectification Plan, the Buyer must within five Working Days of the date of the rejection submit a revised Certification Rectification Plan and Paragraph 7.5.2 will apply to the re-submitted plan;

7.5.4 the rejection by the Buyer of a revised Certification Rectification Plan is a material Default of the Contract; and

7.5.5 if the Buyer accepts the Certification Rectification Plan, the Supplier must start work immediately on the plan.

## 8. Government Data Handled using Supplier Information Management System

8.1 The Supplier acknowledges that the Supplier Information Management System:

8.1.1 is intended only for the Handling of Government Data that is classified as OFFICIAL; and

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

in each case using the Government Security Classification Policy.

8.2 The Supplier must:

8.2.1 not alter the classification of any Government Data; and

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

(a) immediately inform the Buyer; and

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

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

8.3.1 the Expected Behaviours; and

8.3.2 the Security Controls.

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

## 9. Security Management Plan

9.1 This Paragraph 9 applies only where the Buyer has assessed that the Contract is a higher-risk consultancy agreement.

**Preparation of Security Management Plan**

9.2 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 and the Contract in order to ensure the security of the Government Data and the Supplier Information Management System.

9.3 The Supplier shall prepare and submit to the Buyer within [20] Working Days of the Effective Date, the Security Management Plan, which must include:

9.3.1 an assessment of the Supplier Information Management System against the requirements of this Schedule, including Appendix 1;

9.3.2 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 Government Data, the Buyer, the Services and/or users of the Services;

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

9.3.4 the following information in respect of each Sub-contractor:

(a) the Sub-contractor's:

(i) legal name;

(ii) trading name (if any);

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

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

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

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

(e) the measures the Sub-contractor has in place to comply with the requirements of this Schedule.

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

9.4.1 an information security approval statement, which shall confirm that the Supplier may use the Supplier Information Management System to Handle Government Data; or

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

9.5 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 [ten] Working Days of the date of the rejection, or such other period agreed with the Buyer.

**Updating Security Management Plan**

9.6 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**

9.7 The Supplier shall notify the Buyer within [two] Working Days after becoming aware of:

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

9.7.2 a new risk to the components or architecture of the Supplier Information Management System;

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

9.7.4 a change in the threat profile;

9.7.5 a significant change to any risk component;

9.7.6 a significant change in the quantity of Personal Data held within the Service;

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

9.7.8 an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns.

9.8 Within [ten] 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.

## Appendix 1: Security requirements

### 1 Location

1.1 Unless otherwise agreed with the Buyer, the Supplier must, and must ensure that its Sub-contractors must, at all times, store, access or Handle Government Data either:

1.1.1 in the United Kingdom; or

1.1.2 in 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).

1.2 The Supplier must, and must ensure that its Sub-contractors store, access or Handle Government Data in a facility operated by an entity where:

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

1.2.2 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;

1.2.3 the Supplier or Sub-contractor has taken reasonable steps to assure itself that:

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

(b) the Sub-contractor's system has in place appropriate technical and organisational measures to ensure that the Sub-contractor will store, access, manage and/or Handle the Government Data as required by this Schedule; and

1.2.4 the Buyer has not given the Supplier a Prohibition Notice under Paragraph 1.3.

1.3 The Buyer may by notice in writing at any time give notice to the Supplier that it and its Sub-contractors must not undertake or permit to be undertaken, the storage, access or Handling Government Data as specified in the notice (a "**Prohibited Activity**"):

1.3.1 in any particular country or group of countries;

1.3.2 in or using facilities operated by any particular entity or group of entities; and/or

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

1.4 Where the Supplier or Sub-contractor, on the date of the Prohibition Notice undertakes any Relevant Activities 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:

2.1.1 all locations at which Government Data is Handled (**Secure Locations**) have the necessary physical protective security measures in place to prevent unauthorised access, damage and interference, whether malicious or otherwise, to that Government Data; and

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

## 3 Vetting, Training and Staff Access

### Vetting before performing or managing Services

3.1 The Supplier must not engage Supplier Staff, and must ensure that Sub-contractors do not engage Supplier Staff, in any activity relating to the performance and management of the Services unless:

3.1.1 that individual has passed the security checks listed in Paragraph 3.2; or

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

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

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

(a) the individual's identity;

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

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

(d) that the individual has no Relevant Convictions;

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

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

### Exception for certain Sub-contractors

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

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

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

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

**Annual training**

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

3.4.1 general training concerning security and data handling; and

3.4.2 phishing, including the dangers from ransomware and other malware.

**Staff access**

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

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

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

**Remote Working**

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

3.8.1 unless approved in writing by the Buyer, Privileged Users do not undertake Remote Working; and

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

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

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

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

3.9.3 ensure that Supplier Staff undertake Remote Working only in accordance with the Remote Working Policy; and

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

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

3.10.1 restricting or prohibiting Supplier Staff from printing documents in any Remote Location;

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

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

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

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

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

3.10.5 for each different category of Supplier Staff subject to the proposed Remote Working Policy:

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

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

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

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

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

## 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 is stored or Handled in accordance the following requirements:

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

4.1.2 users must authenticate before gaining access;

4.1.3 all Government Data must be encrypted using a encryption tool agreed to by the Buyer;

4.1.4 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;

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

4.1.6 the Suppler or Sub-contractor, as applicable, can, without physical access to the End-user Device, remove or make inaccessible all Government Data on the device and prevent any user or group of users from accessing the device; and

4.1.7 all End-user Devices are within in the scope of any current Cyber Essentials Plus certificate held by the Supplier, or any ISO/IEC 27001:2018 certification issued by a UKAS-Recognised Certification Body (or equivalent certifications), where the scope of that certification includes the Services.

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

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

## 5 Encryption

5.1 Unless Paragraph 5.2 applies, the Supplier must ensure, and must ensure that all Sub-contractors ensure, that Government Data is encrypted:

5.1.1 when stored at any time when no operation is being performed on it; and

5.1.2 when transmitted.

5.2 Where the Supplier, or a Sub-contractor, cannot encrypt Government Data as required by Paragraph 5.1, the Supplier must:

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

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

5.2.3 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.

5.3 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.

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

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

5.4.1 the subset or subsets of Government Data not encrypted and the circumstances in which that will occur; and

5.4.2 the protective measure that the Supplier and/or Sub-contractor will put in please in respect of the unencrypted Government Data.

5.5 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.

**6 Backup and recovery of Government Data**

6.1 The Supplier must ensure that the Supplier System:

9.8.1 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

9.8.2 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.

6.2 The Supplier must ensure the Supplier System:

6.2.1 uses backup location for Government Data that are physically and logically separate from the rest of the Supplier System;

6.2.2 the backup system monitors backups of Government Data to:

(a) identifies any backup failure; and

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

6.2.3 any backup failure is remedied promptly;

6.2.4 the backup system monitors the recovery of Government Data to:

(a) identify any recovery failure; and

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

6.2.5 any recovery failure is promptly remedied.

## 7 Access Control

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

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

7.1.2 require multi-factor authentication for all user accounts that have access to Government Data or that are Privileged Users;

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

7.1.4 maintain records detailing each person's access to the Supplier Information Management System and Sites, and make those records available to the Buyer on request.

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

7.2.1 are accessible only from dedicated End-user Devices;

7.2.2 are configured so that those accounts can only be used for system administration tasks;

7.2.3 require passwords with high complexity that are changed regularly; and

7.2.4 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.

7.3 The Supplier must require, and must ensure that all Sub-contractors require, that Privileged Users use unique and substantially different passwords for their different accounts on the Supplier Information Management System.

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

7.4.1 configure any hardware that forms part of the Supplier Information Management System that is capable of requiring a password before it is accessed to require a password; and

7.4.2 change the default password of that hardware to a password of high complexity that is substantially different from the password required to access similar hardware.

## 8 Malicious Software

8.1 The Supplier shall install and maintain Anti-virus Software or procure that Anti-virus Software is installed and maintained on the Supplier Information Management System.

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

8.2.1 prevents the installation of the most common forms of Malicious Software in the Supplier Information Management System;

8.2.2 is configured to perform automatic software and definition updates;

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

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

8.3 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.

8.4 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 8 is a material Default.

## 9 Security Testing

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

**Note:** the definition of Supplier Information Management System includes those information and communications technology systems that Sub-contractors will use to assist or contribute to the Supplier providing the Services.

9.2 The Supplier must before providing the Services and when reasonably requested by the Buyer, either:

9.2.1 provide details of any security testing undertaken by a CHECK Service Provider in respect of the Supplier Information Management System in the calendar year immediately preceding the Buyer's request or the Effective Date (as appropriate), including:

(a) the parts of the Supplier Information Management System tested;

(b) a full, unedited and unredacted copy of the testing report; and

(c) the remediation plan prepared by the Supplier to address any vulnerabilities disclosed by the security testing; and

(d) the Supplier's progress in implementing that remediation plan; or

9.2.2 where no such testing was undertaken, conduct security testing of the Supplier Information Management System by:

(a) engaging a CHECK Service Provider and ensuring that the CHECK Service Provider uses a qualified CHECK Team Leader and CHECK Team Members to perform the testing;

(b) designing and implementing the testing so as to minimise its impact on the Supplier Information Management System and the delivery of the Services; and

(c) providing the Buyer with a full, unedited and unredacted copy of the testing report without delay and in any event within ten Working Days of its receipt by the Supplier.

9.3 The Supplier must remediate any vulnerabilities classified as "medium" or above in the security testing:

9.3.1 before Handling Buyer data where the vulnerability is discovered before the Supplier begins to Handle Government Data;

9.3.2 where the vulnerability is discovered when the Supplier has begun to Handle Government Data:

(a) by the date agreed with the Buyer; or

(b) where no such agreement is reached:

(i) within five Working Days of becoming aware of the vulnerability and its classification where the vulnerability is classified as critical;

(ii) within one month of becoming aware of the vulnerability and its classification where the vulnerability is classified as high; and

(iii) within three months of becoming aware of the vulnerability and its classification where the vulnerability is classified as medium.

9.4 The Supplier must notify the Buyer immediately if it does not, or considers it will not be able to, remedy the vulnerabilities classified as high or medium in a Security Test report within the time periods specified in Paragraph 9.3.2.

## 10 Breach of Security

10.1 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.

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

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

10.2.2 remedy such Breach of Security to the extent possible;

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

10.2.4 prevent a further Breach of Security in the future which exploits the same root cause failure.

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

10.3.1 notify the Buyer as soon as reasonably practicable after becoming aware of the breach, and in any event within [24] hours;

10.3.2 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;

10.3.3 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

10.3.4 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.

10.4 As soon as reasonably practicable and, in any event, within five Working Days, or such other period agreed with the Buyer, following the Breach of Security or attempted Breach of Security, provide to the Buyer full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Buyer.

10.5 The Supplier must take the steps required by Paragraph 10.2 at its own cost and expense.

## 11 Sub-contractors

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

11.1.1 undertake sufficient due diligence of the proposed Sub-contractor to provide reasonable assurance that the proposed Sub-contractor can perform the obligations that this Schedule requires the Supplier ensure that the proposed Sub-contractor performs;

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

11.1.3 provides those records to the Buyer on request.

## 12 Third-party software and tools

12.1 Before using any software or tool as part of the Supplier Information Management System, the Supplier must:

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

12.1.2 where there are any recognised security vulnerabilities, either:

(a) remedy vulnerabilities; or

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

12.1.3 keep adequate records of the due diligence and efforts to remedy or mitigate identified vulnerabilities; and

12.1.4 provide the Buyer with copies of those records on request.

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

## 13 Deletion and return of Government Data

13.1 The Supplier must, and must ensure that all Sub-contractors, securely erase any or all Government Data held by the Supplier or Sub-contractor when requested to do so by the Buyer using a deletion method that ensures that even a determined expert using specialist techniques can recover only a small fraction of the data deleted.

13.2 Paragraph 13.1 does not apply to Government Data:

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

13.2.2 to which the Supplier has rights to Handle independently from the Contract; or

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

13.3 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:

13.3.1 when requested to do so by the Buyer; and

13.3.2 using the method specified by the Buyer.

`