

## **Schedule 16 (Security)**

# Contents

<b>1 Supplier obligations</b>	<b>4</b>
<b>2 Definitions</b>	<b>6</b>
<b>Part One: Core Requirements</b>	<b>11</b>
<b>3 Certification Requirements</b>	<b>11</b>
<b>4 Location</b>	<b>11</b>
<b>5 Staff vetting</b>	<b>12</b>
<b>6 Supplier assurance letter</b>	<b>12</b>
<b>7 Assurance</b>	<b>12</b>
<b>8 Use of Subcontractors and third parties</b>	<b>13</b>
<b>Part Two: Additional Requirements</b>	<b>14</b>
<b>9 Security testing</b>	<b>14</b>
<b>10 Cloud Security Principles</b>	<b>15</b>
<b>11 Information about Subcontractors, Sites, Third Party Tools and third parties</b>	<b>15</b>
<b>12 Encryption</b>	<b>16</b>
<b>13 Protective monitoring system</b>	<b>17</b>
<b>14 Patching</b>	<b>17</b>
<b>15 Malware protection</b>	<b>18</b>
<b>16 End-user Devices</b>	<b>18</b>
<b>17 Vulnerability scanning</b>	<b>19</b>
<b>18 Access control</b>	<b>19</b>
<b>19 Return and deletion of Government Data</b>	<b>20</b>
<b>20 Physical security</b>	<b>20</b>
<b>21 Breach of security</b>	<b>20</b>
<b>22 Security Management Plan</b>	<b>20</b>



# 1 Supplier obligations

## Core requirements

- 1.1 The Supplier must comply with the core requirements set out in Paragraphs 3 to 8.
- 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:

<b>Certifications</b> (see Paragraph 3)		
The Supplier must have the following Certifications:	ISO/IEC 27001:2013 by a UKAS-approved certification body	X
	Cyber Essentials Plus	<input type="checkbox"/>
	Cyber Essentials	X
Subcontractors that Process Government Data must have the following Certifications:	ISO/IEC 27001:2013 by a UKAS-approved certification body	<input type="checkbox"/>
	Cyber Essentials Plus	<input type="checkbox"/>
	Cyber Essentials	<input type="checkbox"/>
<b>Locations</b> (see Paragraph 4)		
The Supplier and Subcontractors may store, access or Process Government Data in:	the United Kingdom only	<input type="checkbox"/>
	the United Kingdom and European Economic Area only	<input type="checkbox"/>
	anywhere in the world not prohibited by the Buyer	X

## 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.

<b>Security testing</b> (see Paragraph 9)	
The Supplier must undertake security testing at least once every Contract Year and remediate any vulnerabilities, where it is technically feasible to do so	X
<b>Cloud Security Principles</b> (see Paragraph 10)	
The Supplier must assess the Supplier System against the Cloud Security Principles	X
<b>Record keeping</b> (see paragraph 11)	

The Supplier must keep records relating to Subcontractors, Sites, Third Party Tools and third parties	<input type="checkbox"/>
<b>Encryption</b> (see Paragraph 12)	
The Supplier must encrypt Government Data while at rest or in transit	X
<b>Protecting Monitoring System</b> (see Paragraph 13)	
The Supplier must implement an effective Protective Monitoring System	X
<b>Patching</b> (see Paragraph 14)	
The Supplier must patch vulnerabilities in the Supplier System promptly	X
<b>Malware protection</b> (see Paragraph 15)	
The Supplier must use appropriate Anti-virus Software	<input type="checkbox"/>
<b>End-user Devices</b> (see Paragraph 16)	
The Supplier must manage End-user Devices appropriately	<input type="checkbox"/>
<b>Vulnerability scanning</b> (see Paragraph 17)	
The Supplier must scan the Supplier System monthly for unpatched vulnerabilities	X
<b>Access control</b> (see paragraph 18)	
The Supplier must implement effective access control measures for those accessing Government Data and for Privileged Users	X
<b>Return and deletion of Government Data</b> (see Paragraph 19)	
The Supplier must return or delete Government Data when requested by the Buyer	<input type="checkbox"/>
<b>Physical security</b> (see Paragraph 20)	
The Supplier must store Government Data in physically secure locations	<input type="checkbox"/>
<b>Security breaches</b> (see Paragraph 21)	
The Supplier must report any Breach of Security to the Buyer promptly	X
<b>Security Management Plan</b> (see Paragraph 22)	
The Supplier must provide the Buyer with a Security Management Plan detailing how the requirements for the options selected have been met.	<input type="checkbox"/>

## 2 Definitions

<b>“Anti-virus Software”</b>	<p>means software that:</p> <ul style="list-style-type: none"> <li>protects the Supplier System from the possible introduction of Malicious Software;</li> <li>scans for and identifies possible Malicious Software in the Supplier System;</li> <li>if Malicious Software is detected in the Supplier System, so far as possible: <ul style="list-style-type: none"> <li>prevents the harmful effects of the Malicious Software; and</li> <li>removes the Malicious Software from the Supplier System;</li> </ul> </li> </ul>
<b>“Contract Year”</b>	<p>means:</p> <ul style="list-style-type: none"> <li>a period of 12 months commencing on the Effective Date;</li> <li>thereafter a period of 12 months commencing on each anniversary of the Effective Date;</li> <li>with the final Contract Year ending on the expiry or termination of the Term;</li> </ul>
<b>“CREST Service Provider”</b>	<p>means a company with an information security accreditation of a security operations centre qualification from CREST International;</p>
<b>“Government Data”</b>	<p>means any:</p> <ul style="list-style-type: none"> <li>data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media;</li> <li>Personal Data for which the Buyer is a, or the, Data Controller; or</li> <li>any meta-data relating to categories of data referred to in paragraphs (a) or (b);</li> </ul> <p>that is:</p> <ul style="list-style-type: none"> <li>supplied to the Supplier by or on behalf of the Buyer; or</li> <li>that the Supplier generates, processes, stores or transmits under this Agreement; and</li> </ul> <p>for the avoidance of doubt includes the Code and any meta-data relating to the Code.</p>
<b>“Certifications”</b>	<p>means one or more of the following certifications:</p> <ul style="list-style-type: none"> <li>ISO/IEC 27001:2013 by a UKAS-approved certification body in respect of the Supplier System, or in respect of a</li> </ul>

	<p>wider system of which the Supplier System forms part; and</p> <p>Cyber Essentials Plus; and/or</p> <p>Cyber Essentials;</p>
<b>“Breach of Security”</b>	<p>means the occurrence of:</p> <p>any unauthorised access to or use of the Services, the Sites, the Supplier System and/or the Government Data;</p> <p>the loss (physical or otherwise), corruption and/or unauthorised disclosure of any Government Data, including copies of such Government Data; and/or</p> <p>any part of the Supplier System ceasing to be compliant with the required Certifications;</p> <p>the installation of Malicious Software in the Supplier System:</p> <p>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</p> <p>includes any attempt to undertake the activities listed in sub-paragraph (a) where the Supplier has reasonable grounds to suspect that attempt:</p> <p>was part of a wider effort to access information and communications technology operated by or on behalf of Central Government Bodies; or</p> <p>was undertaken, or directed by, a state other than the United Kingdom;</p>
<b>“CHECK Scheme”</b>	<p>means the NCSC’s scheme under which approved companies can conduct authorised penetration tests of public sector and critical national infrastructure systems and networks;</p>
<b>“CHECK Service Provider”</b>	<p>means a company which, under the CHECK Scheme:</p> <p>has been certified by the NCSC;</p> <p>holds “Green Light” status; and</p> <p>is authorised to provide the IT Health Check services required by Paragraph 5.2 (<i>Security Testing</i>);</p>
<b>“Cloud Security Principles”</b>	<p>means the NCSC’s document “Implementing the Cloud Security Principles” as updated or replaced from time to time and found at <a href="https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles">https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles</a>.</p>
<b>“Cyber Essentials”</b>	<p>means the Cyber Essentials certificate issued under the Cyber Essentials Scheme;</p>

<b>“Cyber Essentials Plus”</b>	means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme;
<b>“Cyber Essentials Scheme”</b>	means the Cyber Essentials scheme operated by the NCSC;
<b>“End-user Device”</b>	means any personal computers, laptops, tablets, terminals, smartphones or other portable electronic devices used in the provision of the Services;
<b>“IT Health Check”</b>	means testing of the Supplier Information Management System by a CHECK Service Provider;
<b>“Malicious Software”</b>	means any software program or code intended to destroy, interfere with, corrupt, remove, transmit or cause undesired effects on program files, data or other information, executable code, applications, macros or configurations;
<b>“NCSC”</b>	means the National Cyber Security Centre, or any successor body performing the functions of the National Cyber Security Centre;
<b>“NCSC Device Guidance”</b>	means the NCSC’s document “Device Security Guidance”, as updated or replaced from time to time and found at <a href="https://www.ncsc.gov.uk/collection/device-security-guidance">https://www.ncsc.gov.uk/collection/device-security-guidance</a> ;
<b>“Privileged User”</b>	means a user with system administration access to the Supplier Information Management System, or substantially similar access privileges;
<b>“Process”</b>	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;
<b>“Prohibition Notice”</b>	means the meaning given to that term by Paragraph 4.4.
<b>“Protective Monitoring System”</b>	has the meaning given to that term by Paragraph 13.1;
<b>“Relevant Conviction”</b>	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;
<b>“Sites”</b>	means any premises (including the Buyer’s Premises, the Supplier’s premises or third party premises):  from, to or at which:  the Services are (or are to be) provided; or



	<p>the Supplier manages, organises or otherwise directs the provision or the use of the Services; or</p> <p>where:</p> <p>any part of the Supplier System is situated; or</p> <p>any physical interface with the Authority System takes place;</p>
<b>“Standard Contractual Clauses”</b>	<p>means, for the purposes of this Schedule 16 (Security):</p> <p>the standard data protection paragraphs specified in Article 46 of the UK GDPR setting out the appropriate safeguards for the transmission of personal data outside the combined territories of the United Kingdom and the European Economic Area;</p> <p>as modified to apply equally to the Government Data as if the Government Data were Personal Data;</p>
<b>“Subcontractor Personnel”</b>	<p>means:</p> <p>any individual engaged, directly or indirectly, or employed, by any Subcontractor; and</p> <p>engaged in or likely to be engaged in:</p> <p>the performance or management of the Services; or</p> <p>the provision of facilities or services that are necessary for the provision of the Services;</p>
<b>“Supplier System”</b>	<p>means</p> <p>any:</p> <p>information assets,</p> <p>IT systems,</p> <p>IT services; or</p> <p>Sites,</p> <p>that the Supplier or any Subcontractor will use to Process, or support the Processing of, Government Data and provide, or support the provision of, the Services; and</p> <p>the associated information management system, including all relevant:</p> <p>organisational structure diagrams;</p> <p>controls;</p> <p>policies;</p> <p>practices;</p> <p>procedures;</p> <p>processes; and</p>

	resources;
<b>“Third-party Tool”</b>	means any activity conducted other than by the Supplier during which the Government Data is accessed, analysed or modified, or some form of operation is performed on it;

## **Part One: Core Requirements**

### **3 Certification Requirements**

- 3.1 Where the Buyer has not specified Certifications under Paragraph 1, the Supplier must ensure that it and any Subcontractors that Process Government Data are certified as compliant with Cyber Essentials.
- 3.2 Where the Buyer has specified Certifications under Paragraph 1, the Supplier must ensure that both:
- (a) it; and
  - (b) any Subcontractor that Processes Government Data,
- are certified as compliant with the Certifications specified by the Buyer in Paragraph 1:
- 3.3 The Supplier must ensure that the specified Certifications are in place for it and any relevant Subcontractor:
- (a) before the Supplier or any Subcontractor Processes Government Data; and
  - (b) throughout the Term.

### **4 Location**

- 4.1 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 Process Government Data outside the United Kingdom.
- 4.2 Where the Buyer has specified locations or territories in Paragraph 1, the Supplier must, and ensure that its Subcontractors, at all times store, access or process Government Data only in or from the geographic areas specified by the Buyer.
- 4.3 Where the Buyer has permitted the Supplier and its Subcontractors to store, access or process Government Data outside the United Kingdom or European Economic Area, the Supplier must, and must ensure that its Subcontractors store, access or process 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 Sub-contractors in this Schedule 16 (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 Sub-contractor will store, access, manage and/or Process the Government Data as required by this Schedule 16 (Security);
  - (d) the Buyer has not given the Supplier a Prohibition Notice under Paragraph 4.4.

- 4.4 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 Processing of Government Data in one or more countries or territories (a **"Prohibition Notice"**).
- 4.5 Where the Supplier must and must ensure Subcontractors comply with the requirements of a Prohibition Notice within 40 Working Days of the date of the notice.

## 5 Staff vetting

- 5.1 The Supplier must not allow Supplier Personnel, and must ensure that Subcontractors do not allow Subcontractor Personnel, to access or Process 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 HMG Baseline Personnel Security Standard (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) has not undergone national security vetting clearance to the level specified by the Authority for such individuals or such roles as the Authority may specify

## 6 Supplier assurance letter

- 6.1 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 Agreement;
  - (b) it has fully complied with all requirements of this Schedule 16 (Security); and
  - (c) all Subcontractors have complied with the requirements of this Schedule 16 (Security) with which the Supplier is required to ensure they comply;
  - (d) the Supplier considers that its security and risk mitigation procedures remain effective.

## 7 Assurance

- 7.1 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 Schedule 16 (Security).
- 7.2 The Supplier must provide that information and those documents:

- (a) within 10 Working Days of a request by the Buyer;
- (b) except in the case of original document, in the format and with the content and information required by the Buyer; and
- (c) in the case of original document, as a full, unedited and unredacted copy.

## **8 Use of Subcontractors and third parties**

- 8.1 The Supplier must ensure that Subcontractors and any other third parties that store, have access to or Process Government Data comply with the requirements of this Schedule 16 (Security).

## Part Two: Additional Requirements

### 9 Security testing

9.1 The Supplier must:

- (a) before Processing Government Data;
- (b) at least once during each Contract Year; and

undertake the following activities:

- (c) conduct security testing of the Supplier System (an “**IT Health Check**”) in accordance with Paragraph 9.2; and
- (d) implement any findings, and remedy any vulnerabilities identified by the IT Health Check in accordance with Paragraph 9.3.

9.2 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, Process or manage Government Data; and
- (d) ensure that the IT Health Check provides for effective penetration testing of the Supplier System.

9.3 The Supplier treat any vulnerabilities as follows:

- (a) the Supplier must remedy any vulnerabilities classified as critical 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 technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 9.3(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 technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 9.3(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 Health 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 technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 9.3(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.

## **10 Cloud Security Principles**

- 10.1 The Supplier must ensure that the Supplier Solution complies with the Cloud Security Principles.
- 10.2 The Supplier must assess the Supplier Solution against the Cloud Security Principles to assure itself that it complies with Paragraph 10.1:
- (a) before Processing Government Data;
  - (b) at least once each Contract Year; and
  - (c) when required by the Buyer.
- 10.3 The Supplier must:
- (a) keep records of any assessment that it makes under Paragraph 10.2; and
  - (b) provide copies of those records to the Buyer within 10 Working Days of any request by the Buyer.

## **11 Information about Subcontractors, Sites, Third Party Tools and third parties**

- 11.1 The Supplier must keep the following records:
- (a) for Subcontractors or third parties that store, have access to or Process Government Data:
    - (i) the Subcontractor or third party's name:
      - (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 Relevant 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 Processed 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 Schedule 16 (Security);
  - (b) for Sites from or at which Government Data is accessed or Processed:
    - (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 Relevant Certifications that apply to the Site;
    - (iv) the Government Data stored at, or Processed 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.
- 11.2 The Supplier must update the records it keeps in accordance with Paragraph 11.1:
- (a) at least four times each Contract Year;
  - (b) whenever a Subcontractor, third party that accesses or Processes Government Data, Third Party Tool or Site changes; or
  - (c) whenever required to go so by the Buyer.

11.3 The Supplier must provide copies of the records it keeps in accordance with Paragraph 11.1 to the Buyer within 10 Working Days of any request by the Buyer.

## 12 Encryption

12.1 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.

### **13 Protective monitoring system**

13.1 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 that does;
- (c) identify and implement changes to the Supplier System to prevent future any 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**”).

13.2 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.

### **14 Patching**

14.1 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 technical feasible to patch the vulnerability but not technically feasible to do so as required by Paragraph 14.1(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 technical feasible to patch the vulnerability but not technically feasible to do so as required by Paragraph 14.1(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 technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 14.1(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.

## **15 Malware protection**

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

15.2 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.

## **16 End-user Devices**

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

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

16.2 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 Agreement.

## **17 Vulnerability scanning**

17.1 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 14.

## **18 Access control**

18.1 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.

18.2 The Supplier must ensure, and must ensure that all Subcontractors 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 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.

## **19 Return and deletion of Government Data**

- 19.1 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.

## **20 Physical security**

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

## **21 Breach of security**

- 21.1 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.

## **22 Security Management Plan**

- 22.1 This Paragraph 22 applies only where the Buyer has selected this option in paragraph 1.3.

### *Preparation of Security Management Plan*

- 22.2 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 Agreement in order to ensure the security of the Supplier solution and the Buyer data.
- 22.3 The Supplier shall prepare and submit to the Buyer within 20 Working Days of the date of this Agreement, 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 3.

*Approval of Security Management Plan*

- 22.4 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.
- 22.5 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.
- 22.6 The rejection by the Buyer of a revised Security Management Plan is a material Default of this Agreement.

*Updating Security Management Plan*

- 22.7 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*

- 22.8 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.
- 22.9 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.