

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2024

Call-Off Schedule 9 (Security)

Document Management			
Ver	Date	Version	Author
0.1	July 2023	SQ Stage Version	CCS
0.2	August 2023	Dialogue Stage Version	CCS
0.3	October 2023	Initial Tender Stage Version <i>(No changes from Dialogue Stage Version)</i>	CCS
0.4	November 2023	Final Tender Stage Version <i>(No changes from Initial Tender Stage Version)</i>	CCS
1.0	February 2024	Award Version <i>(No changes from Final Tender Stage Version)</i>	CCS
1.1	September 2024	Framework Variation 1 Version	CCS

What the Supplier must do to ensure that Buyer data and Deliverables are kept secure.

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2024

1 Definitions

1.1 In this Call-Off Schedule 9:

“Anti-Malicious Software”	means software that scans for and identifies possible Malicious Software in the IT Environment;
“Breach of Security”	(a) means the occurrence of: (i) any unauthorised access to or use of the Goods and/or Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or (ii) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract,
“Certification Requirements”	means the information security requirements set out in Paragraph 5;
“Check alignment with”	means any operation which is 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;
“CHECK Service Provider”	means a company which has been certified by the National Cyber Security Centre, holds "Green Light" status and is authorised to provide the IT Health Check services required by Paragraph 6.1;

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2024

“CREST Service Provider”	means a company with a SOC Accreditation 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 National Cyber Security Centre;
“Higher Risk Subcontractor”	means a Key Subcontractor that Processes Government Data.
“Incident Management Process”	means the process which the Supplier shall implement immediately after it becomes aware of a Breach of Security which is intended 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 or Deliverables and which shall be prepared by the Supplier in accordance with Paragraph 3 using the template set out in Annex 3;
“Information Assurance Assessment”	means the set of policies, procedures, systems and processes which the Supplier shall implement, maintain and update in accordance with Paragraph 3 in order to manage, mitigate and, where possible, avoid information security risks including cyber-attacks, hacks, data leaks, Personal Data Breaches and/or theft and which shall be prepared by the Supplier using the template set out in Annex 3 of this Call-Off Schedule 9;
“Information Management System”	<p>means</p> <p>(a) those parts of the Supplier System, and those of the Sites, that the Supplier or its Subcontractors will use to provide the parts of the Services and Deliverables that require Processing Government Data; and</p> <p>(b) the associated information assets and systems (including organisational structure,</p>

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2024

	controls, policies, practices, procedures, processes and resources);
“Information Security Approval Statement”	<p>means a notice issued by the Buyer which sets out the information risks which the Supplier has identified as being associated with using the Information Management System and confirms that:</p> <ul style="list-style-type: none">(a) the Buyer is satisfied that the identified risks have been adequately and appropriately addressed;(b) the Buyer has accepted the residual risks; and(c) the Supplier may use the Information Management System to Process Government Data;
“IT Health Check”	has the meaning given in Paragraph 6.1(a);
“Medium Risk Subcontractor”	means a Subcontractor that Processes Government Data, where that data includes the Personal Data of more than 100 individuals in the period between the first Call-Off Contract Commencement Date and the date on which this Contract terminates;
“Remediation Action Plan”	has the meaning given in Paragraph 6.3(c)(i);
“Required Changes Register”	mean the register within the Security Management Plan which is to be maintained and updated by the Supplier and which shall record each of the changes that the Supplier shall make to the Information Management System and/or the Security Management Plan as a consequence of the occurrence of any of the events set out in Paragraph 4.2 together with the date by which such change shall be implemented and the date on which such change was implemented;
“Risk Register”	is the risk register within the Information Assurance Assessment which is to be prepared and submitted to the Buyer for approval in accordance with Paragraph 3;

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2024

“Security Management Plan”	means the document prepared by the Supplier using the template in Annex 3, comprising: (a) the Information Assurance Assessment; (b) the Required Changes Register; and (c) the Incident Management Process;
Special Category Personal Data	means the categories of Personal Data set out in article 9(1) of the UK GDPR;

1 Introduction

1.1 This Call-Off Schedule 9 sets out:

- (a) the arrangements the Supplier must implement before, and comply with when, providing the Services and performing its other obligations under this Contract to ensure the security of the Government Data and the Information Management System;
- (b) the Certification Requirements applicable to the Supplier and each of those Subcontractors which Processes Government Data;
- (c) the security requirements in Annex 1, with which the Supplier must comply;
- (d) the tests which the Supplier shall conduct on the Information Management System during the Term; and
- (e) the Supplier's obligations to:
 - (i) return or destroy Government Data on the expiry or earlier termination of this Contract; and
 - (ii) prevent the introduction of Malicious Software into the Supplier System and to scan for, contain the spread of, and minimise the impact of Malicious Software which is introduced into the Supplier System in Paragraph 8; and
 - (iii) report Breaches of Security to the Buyer.

2 Principles of Security

2.1 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:

- (a) the Sites;
- (b) the IT Environment;

Framework Ref: RM6288

Variation 1 Version

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2024

- (c) the Information Management System; and
 - (d) the Services and Deliverables.
- 2.2 Notwithstanding the involvement of the Buyer in assessing the arrangements which the Supplier implements to ensure the security of the Government Data and the Information Management System, the Supplier shall be, and shall remain, responsible for:
 - (a) the security, confidentiality, integrity and availability of the Government Data whilst that Government Data is under the control of the Supplier or any of its Subcontractors; and
 - (b) the security of the Information Management System.
- 2.3 The Supplier shall:
 - (a) comply with the security requirements in Annex 1; and
 - (b) ensure that each Subcontractor that Processes Government Data complies with the Subcontractor Security Requirements.
- 2.4 The Supplier shall provide the Buyer with access to Supplier Staff responsible for information assurance to facilitate the Buyer's assessment of the Supplier's compliance with its obligations set out in this Call-Off Schedule 9 at reasonable times on reasonable notice.

3 Information Security Approval Statement

- 3.1 The Supplier must ensure that its Implementation Plan sets out in sufficient detail how it will ensure compliance with the requirements of this Call-Off Schedule 9, including any requirements imposed on Subcontractors by Annex 2, from the Call-Off Contract Commencement Date.
- 3.2 The Supplier may not use the Information Management System to Process Government Data unless and until:
 - (a) the Supplier has procured the conduct of an IT Health Check of the Supplier System by a CHECK Service Provider or a CREST Service Provider in accordance with Paragraph 6.1; and
 - (b) the Buyer has issued the Supplier with an Information Security Approval Statement in accordance with the process set out in this Paragraph 3.
- 3.3 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 and the Contract in order to ensure the security of the Government Data and the Information Management System.

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2024

- 3.4 The Supplier shall prepare and submit to the Buyer within twenty (20) Working Days of the date of this Contract, the Security Management Plan, which comprises:
- (a) an Information Assurance Assessment;
 - (b) the Required Changes Register; and
 - (c) the Incident Management Process.
- 3.5 The Buyer shall review the Supplier's proposed Security Management Plan as soon as possible and, in any event within twenty (20) Working Days of receipt and shall either issue the Supplier with:
- (a) an Information Security Approval Statement, which shall confirm that the Supplier may use the Information Management System to Process Government Data; or
 - (b) a rejection notice, which shall set out the Buyer's reasons for rejecting the Security Management Plan.
- 3.6 If the Buyer rejects the Supplier's proposed Security Management Plan, the Supplier shall take the Buyer's reasons into account in the preparation of a revised Security Management Plan, which the Supplier shall submit to the Buyer for review within ten (10) Working Days or such other timescale as agreed with the Buyer.
- 3.7 The Buyer may require, and the Supplier shall provide the Buyer and its authorised representatives with:
- (a) access to the Supplier Staff;
 - (b) access to the Information Management System to audit the Supplier and its Subcontractors' compliance with this Contract; and
 - (c) 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 Subcontractors have implemented in order to ensure the security of the Government Data and the Information Management System are consistent with the representations in the Security Management Plan. The Supplier shall provide the access required by the Buyer in accordance with this Paragraph within ten (10) 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 twenty four (24) hours of receipt of such request.

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2024

4 Compliance Reviews

- 4.1 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.
- 4.2 The Supplier shall notify the Buyer within two (20) Working Days after becoming aware of:
- (a) a significant change to the components or architecture of the Information Management System;
 - (b) a new risk to the components or architecture of the Information Management System;
 - (c) a vulnerability to the components or architecture of the Service which is classified 'Medium', 'High', 'Critical' or 'Important' in accordance with the classification methodology set out in Paragraph 9.2 of Annex 1 to this Call-Off Schedule 9;
 - (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 ISO/IEC 27001 (at least ISO/IEC 27001:2013) audit report produced in connection with the Certification Requirements indicates significant concerns.
- 4.3 Within ten (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 Required Changes Register and submit the updated Required Changes Register the Buyer for review and approval.
- 4.4 Where the Supplier is required to implement a change, including any change to the Information Management System, the Supplier shall effect such change at its own cost and expense.

5 Certification Requirements

- 5.1 The Supplier shall be certified as compliant with:
- (a) ISO/IEC 27001 (at least ISO/IEC 27001:2013) by a UK Accreditation Service-approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001 (at least ISO/IEC 27001:2013); and

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2024

- (b) Cyber Essentials PLUS,

and shall provide the Buyer with a copy of each such certificate of compliance before the Supplier shall be permitted to receive, store or Process Government Data.
- 5.2 The Supplier shall ensure that each Higher Risk Subcontractor is certified as compliant with either:
 - (a) ISO/IEC 27001 (at least ISO/IEC 27001:2013) by a UK Accreditation Service-approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001 (at least ISO/IEC 27001:2013); or
 - (b) Cyber Essentials PLUS,

and shall provide the Buyer with a copy of each such certificate of compliance before the Higher-Risk Subcontractor shall be permitted to receive, store or Process Government Data.
- 5.3 The Supplier shall ensure that each Medium Risk Subcontractor is certified compliant with Cyber Essentials.
- 5.4 The Supplier shall ensure that the Supplier and each Subcontractor who is responsible for the secure destruction of Government Data:
 - (a) securely destroys Government Data only on Sites which are included within the scope of an existing certification of compliance with ISO/IEC 27001 (at least ISO/IEC 27001:2013);
 - (b) should satisfy the Buyer that their data destruction/deletion practices comply with UK GDPR requirements and follows all relevant NCSC guidance; and
 - (c) must maintain an asset register of all Authority supplied information, data and equipment to ensure Authority assets are returned and/or deleted.
- 5.5 The Supplier shall provide the Buyer with evidence of its and its Subcontractor's compliance with the requirements set out in this Paragraph 5 before the Supplier or the relevant Subcontractor (as applicable) may carry out the secure destruction of any Government Data.
- 5.6 The Supplier shall notify the Buyer as soon as reasonably practicable and, in any event within two (2) Working Days, if the Supplier or any Subcontractor ceases to be compliant with the Certification Requirements and, on request from the Buyer, shall or shall procure that the relevant Subcontractor shall:
 - (a) immediately ceases using the Government Data; and

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2024

- (b) procure that the relevant Subcontractor promptly returns, destroys and/or erases the Government Data in accordance with the requirements set out in this Paragraph.

5.7 The Buyer may agree to exempt, in whole or part, the Supplier or any Subcontractor from the requirements of this Paragraph 5. Any exemption must be in writing to be effective. The Supplier must include the exemption in the Security Management Plan.

6 Security Testing

6.1 The Supplier shall, at its own cost and expense procure and conduct:

- (a) testing of the Information Management System by a CHECK Service Provider or a CREST Service Provider ("**IT Health Check**"); and
- (b) such other security tests as may be required by the Buyer,

6.2 The Supplier shall:

- (a) complete all of the above security tests before:
 - (i) the Supplier submits the Security Management Plan to the Buyer for review in accordance with Paragraph 3; and
 - (ii) before the Supplier is given permission by the Buyer to Process or manage any Government Data; and
- (b) repeat the IT Health Check not less than once every twelve (12) Months during the Term and submit the results of each such test to the Buyer for review in accordance with this Paragraph.

6.3 In relation to each IT Health Check, the Supplier shall:

- (a) agree with the Buyer the aim and scope of the IT Health Check;
- (b) promptly, and no later than ten (10) Working Days, following the receipt of each IT Health Check report, provide the Buyer with a copy of the full report;
- (c) in the event that the IT Health Check report identifies any vulnerabilities, the Supplier shall:
 - (i) prepare a remedial plan for approval by the Buyer (each a "**Remediation Action Plan**") which sets out in respect of each vulnerability identified in the IT Health Check report:
 - (A) how the vulnerability will be remedied;
 - (B) unless otherwise agreed in writing between the Parties, the date by which the vulnerability will be remedied, which must be:

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2024

- (1) within three (3) Months of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of “medium”;
 - (2) within one (1) Month of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of “high”; and
 - (3) within seven (7) Working Days of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of “critical”;
 - (C) the tests which the Supplier shall perform or procure to be performed (which may, at the discretion of the Buyer, include a further IT Health Check) to confirm that the vulnerability has been remedied;
 - (ii) comply with the Remediation Action Plan; and
 - (iii) conduct such further tests on the Service as are required by the Remediation Action Plan to confirm that the Remediation Action Plan has been complied with.
- 6.4 The Supplier shall ensure that any testing which could adversely affect the Supplier System shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such tests shall be agreed in advance with the Buyer.
- 6.5 If any testing conducted by or on behalf of the Supplier identifies a new risk, new threat, vulnerability or exploitation technique that has the potential to affect the security of the Information Management System, the Supplier shall within two (2) Working Days of becoming aware of such risk, threat, vulnerability or exploitation technique provide the Buyer with a copy of the test report and:
- (a) propose interim mitigation measures to vulnerabilities in the Information Management System known to be exploitable where a security patch is not immediately available; and
 - (b) where and to the extent applicable, remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the Supplier System) within the timescales set out in the test report or such other timescales as may be agreed with the Buyer.

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2024

- 6.6 The Supplier shall conduct such further tests of the Supplier System as may be required by the Buyer from time to time to demonstrate compliance with its obligations set out this Call-Off Schedule 9 and the Contract.
- 6.7 The Supplier shall notify the Buyer immediately if it fails to, or believes that it will not, mitigate the vulnerability within the timescales set out in Paragraph 6.3.

7 Security Monitoring and Reporting

- 7.1 The Supplier shall:
- (a) monitor the delivery of assurance activities;
 - (b) maintain and update the Security Management Plan in accordance with Paragraph 4;
 - (c) agree a document which presents the residual security risks to inform the Buyer's decision to give approval to the Supplier to Process and transit the Government Data;
 - (d) monitor security risk impacting upon the operation of the Service;
 - (e) report Breaches of Security in accordance with the approved Incident Management Process;
 - (f) agree with the Buyer the frequency and nature of the security reports to be prepared and submitted by the Supplier to the Buyer within twenty (20) Working Days of Effective Date.

8 Breach of Security

- 8.1 If either party becomes aware of a Breach of Security it shall notify the other in accordance with the Incident Management Process.
- 8.2 The Incident Management Process shall, as a minimum, require the Supplier to do the following upon it becoming aware of a Breach of Security or attempted Breach of Security:
- (a) Immediately take all reasonable steps necessary to:
 - (i) minimise the extent of actual or potential harm caused by such Breach of Security;
 - (ii) remedy such Breach of Security to the extent possible;
 - (iii) apply a tested mitigation against any such Breach of Security; and
 - (iv) prevent a further Breach of Security in the future which exploits the same root cause failure;

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2024

- (b) as soon as reasonably practicable and, in any event, within two (2) Working Days, 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.

- 8.3 In the event that any action is taken in response to a Breach of Security or attempted Breach of Security as a result of non-compliance by the Supplier, its Subcontractors and/or all or any part of the Information Management System with this Contract, then such remedial action shall be completed at no additional cost to the Buyer.

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2024

ANNEX 1: SECURITY REQUIREMENTS

1 Security Classification of Information

- 1.1 If the provision of the Services requires the Supplier to Process Government Data which is classified as:
- (a) OFFICIAL-SENSITIVE, the Supplier shall implement such additional measures as agreed with the Buyer from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards; and/or
 - (b) SECRET or TOP SECRET, the Supplier shall only do so where it has notified the Buyer prior to receipt of such Government Data and the Supplier shall implement additional measures as agreed with the Buyer from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards.

2 End User Devices

- 2.1 The Supplier must manage, and must ensure that all Subcontractors manage, all end-user devices used by the Supplier on which Government Data is Processed in accordance the following requirements:
- 2.1.1 the operating system and any applications that 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;
 - 2.1.2 users must authenticate before gaining access;
 - 2.1.3 all Government Data must be encrypted using an encryption tool agreed to by the Buyer;
 - 2.1.4 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;
 - 2.1.5 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;
 - 2.1.6 the Supplier or Subcontractor, 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;
 - 2.1.7 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 (at least ISO/IEC 27001:2013) certification issued by a

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2024

UKAS-approved certification body, where the scope of that certification includes the Services.

- 2.2 The Supplier must comply, and ensure that all Subcontractors comply, with the recommendations in NCSC Device Guidance, as updated, amended or replaced from time to time, as if those recommendations were incorporated as specific obligations under this Agreement.
- 2.3 Where there any conflict between the requirements of this Call-Off Schedule 9 and the requirements of the NCSC Device Guidance, the requirements of this Call-Off Schedule 9 will take precedence.

3 Encryption

- 3.1 The Supplier must ensure, and must ensure that all Subcontractors ensure, that Government Data is encrypted:
 - 3.1.1 when stored at any time when no operation is being performed on it; and
 - 3.1.2 when transmitted.
- 3.2 Where the Supplier, or a Subcontractor, cannot encrypt Government Data the Supplier must:
 - 3.2.1 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;
 - 3.2.2 provide details of the protective measures the Supplier or Subcontractor (as applicable) proposes to take to provide equivalent protection to the Buyer as encryption; and
 - 3.2.3 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.
- 3.3 The Buyer, the Supplier and, where the Buyer requires, any relevant Subcontractor shall meet to agree appropriate protective measures for the unencrypted Government Data.
- 3.4 Where the Buyer and Supplier reach agreement, the Supplier must update the Security Management Plan to include:
 - 3.4.1 the subset or subsets of Government Data not encrypted and the circumstances in which that will occur; and
 - 3.4.2 the protective measure that the Supplier and/or Subcontractor will put in place in respect of the unencrypted Government Data.

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2024

- 3.5 Where the Buyer and Supplier do not reach agreement within forty (40) Working Days of the date on which the Supplier first notified the Buyer that it could not encrypt certain Government Data, follow the process set out in Clause 34 of the Core Terms (Resolving Disputes).

4 Personnel Security

- 4.1 All Supplier Staff shall be subject to a pre-employment check before they may participate in the provision and or management of the Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; verification of the individual's criminal record in accordance with Call-Off Schedule 18 (Background Checks).
- 4.2 The Buyer and the Supplier shall review the roles and responsibilities of the Supplier Staff who will be involved in the management and/or provision of the Services in order to enable the Buyer to determine which roles require additional vetting and a specific national security vetting clearance (e.g. a Counter Terrorist Check; a Security Check). Roles which are likely to require additional vetting and a specific national security vetting clearance include system administrators whose role would provide those individuals with privileged access to IT systems which Process Government Data or data which, if it were Government Data, would be classified as OFFICIAL-SENSITIVE.
- 4.3 The Supplier shall not permit Supplier Staff who fail the security checks required by Paragraphs 4.1 and 4.2 to be involved in the management and/or provision of the Services except where the Buyer has expressly agreed in writing to the involvement of the named individual in the management and/or provision of the Services.
- 4.4 The Supplier shall ensure that Supplier Staff are only granted such access to Government Data as is necessary to enable the Supplier Staff to perform their role and to fulfil their responsibilities.
- 4.5 The Supplier shall ensure that Supplier Staff who no longer require access to the Government Data (e.g. they cease to be employed by the Supplier or any of its Subcontractors), have their rights to access the Government Data revoked within one (1) Working Day.
- 4.6 The Supplier shall ensure that Supplier Staff that have access to the Sites, the IT Environment or the Government Data receive regular training on security awareness that reflects the degree of access those individuals have to the Sites, the IT Environment or the Government Data.
- 4.7 The Supplier shall ensure that the training provided to Supplier Staff under Paragraph 4.6 includes training on the identification and reporting fraudulent communications intended to induce individuals to disclose Personal Data or

Framework Ref: RM6288

Variation 1 Version

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2024

any other information that could be used, including in combination with other Personal Data or information, or with other techniques, to facilitate unauthorised access to the Sites, the IT Environment or the Government Data ("phishing").

5 Identity, Authentication and Access Control

5.1 The Supplier shall operate an access control regime to ensure:

- (a) all users and administrators of the Supplier System are uniquely identified and authenticated when accessing or administering the Services; and
- (b) all persons who access the Sites are identified and authenticated before they are allowed access to the Sites.

5.2 The Supplier shall apply the 'principle of least privilege' when allowing persons access to the Supplier System and Sites so that such persons are allowed access only to those parts of the Sites and the Supplier System they require.

5.3 The Supplier shall retain records of access to the Sites and to the Supplier System and shall make such record available to the Buyer on request.

6 Data Destruction or Deletion

6.1 The Supplier shall:

- (a) prior to securely sanitising any Government Data or when requested the Supplier shall provide the Government with all Government Data in an agreed open format;
- (b) have documented processes to ensure the availability of Government Data in the event of the Supplier ceasing to trade;
- (c) securely erase in a manner agreed with the Buyer any or all Government Data held by the Supplier when requested to do so by the Buyer;
- (d) securely destroy in a manner agreed with the Buyer all media that has held Government Data at the end of life of that media in accordance with any specific requirements in this Contract and, in the absence of any such requirements, as agreed by the Buyer; and
- (e) implement processes which address the CPNI and NCSC guidance on secure sanitisation.

7 Audit and Protective Monitoring

7.1 The Supplier shall collect audit records which relate to security events in the Information Management System or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum)

Framework Ref: RM6288

Variation 1 Version

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2024

include regular reports and alerts setting out details of access by users of the Information Management System, to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of Government Data.

- 7.2 The Supplier and the Buyer shall work together to establish any additional audit and monitoring requirements for the Information Management System.
- 7.3 The retention periods for audit records and event logs must be agreed with the Buyer and documented in the Security Management Plan.

8 Location of Government Data

- 8.1 The Supplier shall not and shall procure that none of its Subcontractors Process Government Data outside the UK or EU without the prior written consent of the Buyer, which may be subject to conditions.

9 Vulnerabilities and Corrective Action

- 9.1 The Buyer and the Supplier acknowledge that from time to time vulnerabilities in the Information Management System will be discovered which unless mitigated will present an unacceptable risk to the Government Data.
- 9.2 The severity of vulnerabilities for COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the agreed method in the Security Management Plan and using the appropriate vulnerability scoring systems including:
- (a) the 'National Vulnerability Database' 'Vulnerability Severity Ratings': 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS scores as set out by NIST at <http://nvd.nist.gov/cvss.cfm>); and
 - (b) Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.
- 9.3 Subject to Paragraph 9.4, the Supplier shall procure the application of security patches to vulnerabilities in the Information Management System within:
- (a) seven (7) days after the public release of patches for those vulnerabilities categorised as 'Critical';
 - (b) thirty (30) days after the public release of patches for those vulnerabilities categorised as 'Important'; and
 - (c) sixty (60) days after the public release of patches for those vulnerabilities categorised as 'Other'.
- 9.4 The timescales for applying patches to vulnerabilities in the Information Management System set out in Paragraph 9.3 shall be extended where:

Framework Ref: RM6288

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2024

- (a) the Supplier can demonstrate that a vulnerability in the Information Management System is not exploitable within the context of the Services (e.g. because it resides in a Software component which is not involved in running in the Services) provided such vulnerabilities shall be remedied by the Supplier within the timescales set out in Paragraph 9.3 if the vulnerability becomes exploitable within the context of the Services;
- (b) the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of five (5) days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Buyer; or
- (c) the Buyer agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the Security Management Plan.

9.5 The Security Management Plan shall include provisions for major version upgrades of all COTS Software to be kept up to date such that all COTS Software are always in mainstream support throughout the Term unless otherwise agreed by the Buyer in writing. All COTS Software should be no more than N-1 versions behind the latest software release.

10 Secure Architecture

10.1 The Supplier shall design the Information Management System in accordance with:

- (a) the NCSC "Security Design Principles for Digital Services", a copy of which can be found at:
<https://www.ncsc.gov.uk/guidance/security-design-principles-digital-services-main>;
- (b) the NCSC "Bulk Data Principles", a copy of which can be found at
<https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main>; and
- (c) the NSCS "Cloud Security Principles", a copy of which can be found at: <https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles> and which are summarised below:
 - (i) "Cloud Security Principle 1: data in transit protection" which, amongst other matters, requires that user data transiting networks should be adequately protected against tampering and eavesdropping;
 - (ii) "Cloud Security Principle 2: asset protection and resilience" which, amongst other matters, requires that user data, and

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2024

the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure;

- (iii) "Cloud Security Principle 3: separation between users" which, amongst other matters, requires that a malicious or compromised user of the service should not be able to affect the service or data of another;
- (iv) "Cloud Security Principle 4: governance framework" which, amongst other matters, requires that the Supplier should have a security governance framework which coordinates and directs its management of the Services and information within it;
- (v) "Cloud Security Principle 5: operational security" which, amongst other matters, requires that the Services need to be operated and managed securely in order to impede, detect or prevent a Breach of Security;
- (vi) "Cloud Security Principle 6: personnel security" which, amongst other matters, requires that where Supplier Staff have access to Government Data and/or the Buyer System that those personnel be subject to appropriate security screening and regular security training;
- (vii) "Cloud Security Principle 7: secure development" which, amongst other matters, requires that the Services be designed and developed to identify and mitigate threats to their security;
- (viii) "Cloud Security Principle 8: supply chain security" which, amongst other matters, requires the Supplier to ensure that appropriate security controls are in place with its Subcontractors and other suppliers;
- (ix) "Cloud Security Principle 9: secure user management" which, amongst other matters, requires the Supplier to make the tools available for the Buyer to securely manage the Buyer's use of the Service;
- (x) "Cloud Security Principle 10: identity and authentication" which, amongst other matters, requires the Supplier to implement appropriate controls in order to ensure that access to Service interfaces is constrained to authenticated and authorised individuals;
- (xi) "Cloud Security Principle 11: external interface protection" which, amongst other matters, requires that all external or less trusted interfaces with the Services should be identified and appropriately defended;

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2024

- (xii) "Cloud Security Principle 12: secure service administration" which, amongst other matters, requires that any ICT system which is used for administration of a cloud service will have highly privileged access to that service;
- (xiii) "Cloud Security Principle 13: audit information for users" which, amongst other matters, requires the Supplier to be able to provide the Buyer with the audit records it needs to monitor access to the Service and the Government Data held by the Supplier and/or its Subcontractors; and
- (xiv) "Cloud Security Principle 14: secure use of the service" which, amongst other matters, requires the Supplier to educate Supplier Staff on the safe and secure use of the Information Management System.

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2024

ANNEX 2: SECURITY REQUIREMENTS FOR SUBCONTRACTORS

1 Application of Annex

- 1.1 This Annex applies to all Subcontractors that Process Government Data.
- 1.2 The Supplier must:
 - (a) ensure that those Subcontractors comply with the provisions of this Annex;
 - (b) keep sufficient records to demonstrate that compliance to the Buyer; and
 - (c) ensure that its Implementation Plan includes Deliverable Items, Milestones and Milestone Dates that relate to the design, implementation and management of any systems used by Subcontractors to Process Government Data.

2 Designing and managing secure solutions

- 2.1 The Subcontractor shall implement their solution(s) to mitigate the security risks in accordance with the NCSC's Cyber Security Design Principles <https://www.ncsc.gov.uk/collection/cyber-security-design-principles>.
- 2.2 The Subcontractor must assess their systems against the NCSC Cloud Security Principles: <https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles> at their own cost and expense to demonstrate that the people, process, technical and physical controls have been delivered in an effective way. The Subcontractor must document that assessment and make that documentation available to the Buyer on the Buyer's request.

3 Data Processing, Storage, Management and Destruction

- 3.1 The Subcontractor must not Process any Government Data outside the UK and EU. The Buyer may permit the Subcontractor to Process Government Data outside the UK and EU and may impose conditions on that permission, with which the Subcontractor must comply. Any permission must be in writing to be effective.
- 3.2 The Subcontractor must when requested to do so by the Buyer:
 - (a) securely destroy Government Data only on Sites which are included within the scope of an existing certification of compliance with ISO/IEC 27001 (at least ISO/IEC 27001:2013);
 - (b) satisfy the Buyer that their data destruction/deletion practices comply with UK GDPR requirements and follows all relevant NCSC guidance; and

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2024

- (c) maintain an asset register of all Authority supplied information, data and equipment to ensure Authority assets are returned and/or deleted.

4 Personnel Security

- 4.1 The Subcontractor must perform appropriate checks on their staff before they may participate in the provision and or management of the Services. Those checks must include all pre-employment checks required by the HMG Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; verification of the individual's employment history; and verification of the individual's criminal record. The HMG Baseline Personnel Security Standard is at <https://www.gov.uk/government/publications/government-baseline-personnel-security-standard>.
- 4.2 The Subcontractor must, if the Buyer requires, at any time, ensure that one or more of the Subcontractor's staff obtains Security Check clearance in order to Process Government Data containing Personal Data above certain volumes specified by the Buyer, or containing Special Category Personal Data.
- 4.3 Any Subcontractor staff who will, when performing the Services, have access to a person under the age of 18 years must undergo Disclosure and Barring Service checks.

5 End User Devices

- 5.1 The Supplier must manage, and must ensure that all Subcontractors manage, all end-user devices used by the Supplier on which Government Data is Processed in accordance the following requirements:
 - (a) the operating system and any applications that 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 an encryption tool agreed to by the Buyer;
 - (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;
 - (f) the Supplier or Subcontractor, as applicable, can, without physical access to the end-user device, remove or make inaccessible all

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2024

Government Data on the device and prevent any user or group of users from accessing the device;

- (g) 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 (at least ISO/IEC 27001:2013) certification issued by a UKAS-approved certification body, where the scope of that certification includes the Services.

5.2 The Supplier must comply, and ensure that all Subcontractors comply, with the recommendations in NCSC Device Guidance, as updated, amended or replaced from time to time, as if those recommendations were incorporated as specific obligations under this Agreement.

5.3 Where there any conflict between the requirements of this Call-Off Schedule 9 and the requirements of the NCSC Device Guidance, the requirements of this Call-Off Schedule 9 will take precedence.

6 Encryption

6.1 The Supplier must ensure, and must ensure that all Subcontractors ensure, that Government Data is encrypted:

- (a) when stored at any time when no operation is being performed on it; and
- (b) when transmitted.

6.2 Where the Supplier, or a Subcontractor, cannot encrypt Government Data the Supplier must:

- (a) immediately inform the Buyer of the subset or subsets of Government Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;
- (b) provide details of the protective measures the Supplier or Subcontractor (as applicable) proposes to take to provide equivalent protection to the Buyer as encryption; and
- (c) provide the Buyer with such information relating to the Government Data concerned, the reasons why that Government Data cannot be encrypted and the proposed protective measures as the Buyer may require.

6.3 The Buyer, the Supplier and, where the Buyer requires, any relevant Subcontractor shall meet to agree appropriate protective measures for the unencrypted Government Data.

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

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2024

- (a) the subset or subsets of Government Data not encrypted and the circumstances in which that will occur; and
- (b) the protective measure that the Supplier and/or Subcontractor will put in place in respect of the unencrypted Government Data.

6.5 Where the Buyer and Supplier do not reach agreement within forty (40) Working Days of the date on which the Supplier first notified the Buyer that it could not encrypt certain Government Data, the parties will follow the process set out in Clause 34 of the Core Terms (Resolving Disputes).

7 Patching and Vulnerability Scanning

7.1 The Subcontractor must proactively monitor supplier vulnerability websites and ensure all necessary patches and upgrades are applied to maintain security, integrity and availability in accordance with the NCSC Cloud Security Principles.

8 Third Party Subcontractors

8.1 The Subcontractor must not transmit or disseminate the Government Data to any other person unless specifically authorised by the Buyer. Such authorisation must be in writing to be effective and may be subject to conditions.

8.2 The Subcontractor must not, when performing any part of the Services, use any software to Process the Government Data where the licence terms of that software purport to grant the licensor rights to Progress the Government Data greater than those rights strictly necessary for the use of the software

ANNEX 3: SECURITY MANAGEMENT PLAN TEMPLATE

Security Management Plan Template

[Project/Service and Supplier Name]

1 Executive Summary

<This section should contain a brief summary of the business context of the system, any key IA controls, the assurance work done, any off-shoring considerations and any significant residual risks that need acceptance.>

2 System Description

2.1 Background

< A short description of the project/product/system. Describe its purpose, functionality, aim and scope.>

2.2 Organisational Ownership/Structure

<Who owns the system and operates the system and the organisational governance structure. This should include how any ongoing security management is integrated into the project governance e.g. how a Security Working Group reports to the project board.>

2.3 Information assets and flows

<The information assets processed by the system which should include a simple high level diagram on one page. Include a list of the type and volumes of data that will be processed, managed and stored within the supplier system. If personal data, please include the fields used such as name, address, department DOB, NI number etc.>

2.4 System Architecture

<A description of the physical system architecture, to include the system management. A diagram will be needed here>

2.5 Users

<A brief description of the system users, to include HMG users as well as any service provider users and system managers. If relevant, security clearance level requirements should be included.>

2.6 Locations

<Where the data assets are stored and managed from. If any locations hold independent security certifications (e.g. ISO27001 (at least ISO/IEC 27001:2013) these should be noted. Any off-shoring considerations should be detailed.>

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

2.7 Test and Development Systems

<Include information about any test and development systems, their locations and whether they contain live system data.>

2.8 Key roles and responsibilities

<A brief description of the lead security roles such as that of the SIRO, IAO, Security manager, Accreditor >

3 Risk Assessment

3.1 Accreditation/Assurance Scope

<This section describes the scope of the Accreditation/Assurance for the system. The scope of the assurance assessment should be clearly indicated, with components of the architecture upon which reliance is placed but assurance will not be done clearly shown e.g. a cloud hosting service. A logical diagram should be used along with a brief description of the components.>

3.2 Risk appetite

<A risk appetite should be agreed with the SRO and included here.>

3.3 Business impact assessment

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

3.4 Risk assessment

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

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

Risk ID	Inherent risk	Inherent risk level	Vulnerability	Controls	Residual risk level
R1	Internet attackers could hack the system.	Medium	The service systems are exposed to the internet via the web portal.	C1: Internet-facing firewalls C2: Internet-facing IP whitelist C3: System hardening C4: Protective monitoring C5: Application access control C16: Anti-virus for incoming files C54: Files deleted when processed C59: Removal of departmental identifier	Very low
R2	Remote attackers could intercept or disrupt information crossing the internet.	Medium	File sharing with organisations across the internet.	C9: TLS communications C10: PGP file-sharing	Very low
R3	Internal users could maliciously or accidentally	Medium-High	Users bank details can be altered as part of the normal business function.	C12. System administrators hold SC clearance.	Low

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

Risk ID	Inherent risk	Inherent risk level	Vulnerability	Controls	Residual risk level
	alter bank details.			C13. All changes to user information are logged and audited. C14. Letters are automatically sent to users' home addresses when bank details are altered. C15. Staff awareness training	

3.5 Controls

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

ID	Control title	Control description	Further information and assurance status
C1	Internet-facing firewalls	Internet-facing firewalls are in place between the internet and the system', which restrict access from the internet to the required ports only.	Assured via ITHC firewall rule check
C2	Internet-facing IP whitelist	An IP whitelist is in place for all access from the internet.	Assured via ITHC

Framework Ref: RM6288

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

C1 5	Staff awareness training	All staff must undertake annual security awareness training and this process is audited and monitored by line managers.	Assured as part of ISO/IEC 27001 (at least ISO/IEC 27001:2013) certification
---------	--------------------------	---	--

3.6 Residual risks and actions

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

4 In-service controls

< This section should describe the controls relating to the information lifecycle, including development, testing, in-service, termination and on-going risk management and accreditation assurance. Details of any formal assurance requirements specified in the contract such as security CHECK testing or maintained ISO/IEC 27001 (at least ISO/IEC 27001:2013) certification should be included. This section should include at least:

- (a) information risk management and timescales and triggers for a review;*
- (b) contractual patching requirements and timescales for the different priorities of patch;*
- (c) protective monitoring arrangements to include how anomalous behaviour is identified and acted upon as well as how logging and auditing of user activity is done;*
- (d) configuration and change management;*
- (e) incident management;*
- (f) vulnerability management;*
- (g) user access management; and*
- (h) data sanitisation and disposal.>*

5 Security Operating Procedures (SyOPs)

< If needed any SyOps requirements should be included and referenced here.>

6 Major Hardware and Software and end of support dates

Framework Ref: RM6288

Variation 1 Version

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

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

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

7 Incident Management Process

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

8 Security Requirements for User Organisations

<Any security requirements for connecting organisations or departments should be included or referenced here.>

9 Required Changes Register

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

Ref	Section	Change	Agreed With	Date agreed	Documentation update	Status
1	6.4	A new Third Party supplier XXXX will be performing the print capability.	Authority name	11/11/2018	Jul-2019	Open

10 Subcontractors

<This should include a table which shows for each Subcontractor their name, the function that they are performing, the data and data volume being processed, the location, and their certification status>

11 Annex A. ISO/IEC 27001 (at least ISO/IEC 27001:2013) and/or Cyber Essential Plus certificates

<Any certifications relied upon should have their certificates included>

12 Annex B. Cloud Security Principles assessment

Framework Ref: RM6288

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

<A spreadsheet may be attached>

13 Annex C. Protecting Bulk Data assessment if required by the Buyer/Customer

<A spreadsheet may be attached>

14 Annex D. Latest ITHC report and Remediation Action Plan