

Schedule 5

Security Management

Part 1: Security Assurance

1 General Application

1.1 It is acknowledged by the Authority that:

[REDACTED]

1.2 [REDACTED]

1.3 Application of Specific Parts: Part 1 (Security Assurance) of this Schedule 5 shall only apply to the cloud-based Operational Services.

2 Definitions

In this Schedule the definitions in Schedule 1 (Definitions) shall apply.

3 Introduction

3.1 This Part 1 of this Schedule sets out:

3.1.1 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 Authority Data and the Information Management System;

3.1.2 the Certification Requirements applicable to the Supplier and each of those Sub-contractors which Processes Authority Data;

3.1.3 the security requirements in Appendix A of Part 1 of this Schedule, with which the Supplier must comply;

3.1.4 the tests which the Supplier shall conduct on the Information Management System during the Term; and

3.1.5 the Supplier's obligations to:

(a) return or destroy Authority Data on the expiry or earlier termination of this Contract; and

(b) 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 10; and

(c) report Breaches of Security to the Authority.

4 Principles of Security

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

4.1.1 the Sites;

4.1.2 the IT Environment;

4.1.3 the Information Management System; and

- 4.1.4 the Services.
- 4.2 Notwithstanding the involvement of the Authority in assessing the arrangements which the Supplier implements to ensure the security of the Authority Data and the Information Management System, the Supplier shall be, and shall remain, responsible for:
 - 4.2.1 the security, confidentiality, integrity and availability of the Authority Data whilst that Authority Data is under the control of the Supplier or any of its Sub-contractors; and
 - 4.2.2 the security of the Information Management System.
- 4.3 The Supplier shall:
 - 4.3.1 Comply with the security requirements in Appendix A of Part 1 of this Schedule; and
 - 4.3.2 ensure that each Sub-contractor that Processes Authority Data complies with the Sub-contractor Security Requirements in Appendix B of Part 1 of this Schedule.
- 4.4 The Supplier shall provide the Authority with access to Supplier Personnel responsible for information assurance to facilitate the Authority's assessment of the Supplier's compliance with its obligations set out in this Schedule at reasonable times on reasonable notice.
- 5 Information Security Approval Statement
 - 5.1 The Supplier must ensure that its Implementation Plan sets out in sufficient detail how it will ensure compliance with the requirements of this Schedule, including any requirements imposed on Sub-contractors by Appendix B of Part 1, from the first Operational Services Commencement Date.
 - 5.2 The Supplier may not use the Information Management System to Process Authority Data unless and until:
 - 5.2.1 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 8.1; and
 - 5.2.2 the Authority has issued the Supplier with an Information Security Approval Statement in accordance with the process set out in this Paragraph 5.
 - 5.3 The Supplier shall document in the Security Management Plan how the Supplier and its Sub-contractors shall comply with the requirements set out in this Schedule and the Contract in order to ensure the security of the Authority Data and the Information Management System.
 - 5.4 The Supplier shall prepare and submit to the Authority within thirty (30) Working Days of the date of this Contract, the Security Management Plan, which comprises:
 - 5.4.1 an Information Assurance Assessment;
 - 5.4.2 the Required Changes Register; and
 - 5.4.3 the Incident Management Process.
 - 5.5 The Authority shall review the Supplier's proposed Security Management Plan as soon as possible and, in any event within thirty (30) Working Days of receipt and shall either issue the Supplier with:
 - 5.5.1 an Information Security Approval Statement, which shall confirm that the Supplier may use the Information Management System to Process Authority Data; or
 - 5.5.2 a rejection notice, which shall set out the Authority's reasons for rejecting the Security Management Plan.

5.6 If the Authority rejects the Supplier's proposed Security Management Plan, the Supplier shall take the Authority's reasons into account in the preparation of a revised Security Management Plan, which the Supplier shall submit to the Authority for review within fifteen (15) Working Days or such other timescale as agreed with the Authority.

5.7 The Authority may require, and the Supplier shall provide the Authority and its authorised representatives with:

5.7.1 access to the Supplier Personnel;

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

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

to assist the Authority to establish whether the arrangements which the Supplier and its Sub-contractors have implemented in order to ensure the security of the Authority 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 Authority 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 Authority with the access that it requires within 24 hours of receipt of such request.

6 Compliance reviews

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

6.2 Save for in respect of Supplier A where a Service warranty as set out in Schedule 34 (ERP Supplier Terms) applies, the Supplier shall notify the Authority within seven (7) Working Days after becoming aware of:

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

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

6.2.3 a vulnerability to the components or architecture of the Service which is classified "Medium", "High" or "Critical" in accordance with the classification methodology set out in Paragraph 9.2 of Appendix A to Part 1 of this Schedule;

6.2.4 a change in the threat profile;

6.2.5 a significant change to any risk component;

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

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

6.2.8 an ISO/IEC 27001 audit report produced in connection with the Certification Requirements indicates significant concerns.

6.3 Within ten (10) Working Days of such notifying the Authority or such other timescale as may be agreed with the Authority, the Supplier shall make the necessary changes to the Required Changes Register and submit the updated Required Changes Register to the Authority for review and approval within such timescale as may be agreed by the Parties, acting reasonably.

- 6.4 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.
- 7 Certification Requirements
- 7.1 The Supplier shall be certified as compliant with:
- 7.1.1 ISO/IEC 27001 by a UK Accreditation Service (UKAS)-approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001; and
- 7.1.2 Cyber Essentials Plus,
- and shall provide the Authority with a copy of each such certificate of compliance before the Supplier shall be permitted to receive, store or Process Authority Data.
- 7.2 The Supplier shall ensure that each Higher Risk Sub-contractor is certified as compliant with either:
- 7.2.1 ISO/IEC 27001 by a UK Accreditation Service-approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001; or
- 7.2.2 Cyber Essentials Plus,
- and shall provide the Authority with a copy of each such certificate of compliance before the Higher-Risk Sub-contractor shall be permitted to receive, store or Process Authority Data.
- 7.3 The Supplier shall ensure that each Sub-contractor is certified compliant with Cyber Essentials.
- 7.4 The Supplier shall ensure that the Supplier and each Sub-contractor who is responsible for the secure destruction of Authority Data:
- 7.4.1 securely destroys Authority Data only on Sites which are included within the scope of an existing certification of compliance with ISO/IEC 27001;
- 7.4.2 should satisfy the Authority that their data destruction/deletion practices comply with UK GDPR requirements and follows all relevant NCSC guidance; and
- 7.4.3 must maintain an asset register of all Authority supplied information, data and equipment to ensure Authority assets are returned and/or deleted.
- 7.5 The Supplier shall provide the Authority with evidence of its and its Sub-contractor's compliance with the requirements set out in this Paragraph 7 before the Supplier or the relevant Sub-contractor (as applicable) may carry out the secure destruction of any Authority Data.
- 7.6 The Supplier shall notify the Authority as soon as reasonably practicable and, in any event within two (2) Working Days, if the Supplier or any Sub-contractor ceases to be compliant with the Certification Requirements and, on request from the Authority, shall or shall procure that the relevant Sub-contractor shall:
- 7.6.1 immediately cease using the Authority Data; and
- 7.6.2 procure that the relevant Sub-contractor promptly returns, destroys and/or erases the Authority Data in accordance with the requirements set out in this Paragraph.
- 7.7 The Authority may agree to exempt, in whole or part, the Supplier or any Sub-contractor from the requirements of this Paragraph 7. Any exemption must be in writing to be effective. The Supplier must include the exemption in the Security Management Plan.

- 8 Security testing
- 8.1 The Supplier shall, at its own cost and expense procure and conduct:
- 8.1.1 testing of the Information Management System by a CHECK Service Provider or a CREST Service Provider (**IT Health Check**); and
- 8.1.2 such other security tests as may be required by the Authority, whereby the Authority acting reasonably agrees only to rely upon its rights under this paragraph 8.1.2 where it has a legitimate reason to do so.
- 8.2 The Supplier shall:
- 8.2.1 complete all of the above security tests before the Supplier is given permission by the Authority to Process or manage any Authority Data; and
- 8.2.2 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 Authority for review in accordance with this Paragraph.
- 8.2.3 re-submit the Security Management Plan to the Authority for review once all of the above security tests have been completed.
- 8.3 In relation to each IT Health Check, the Supplier shall:
- 8.3.1 agree with the Authority the aim and scope of the IT Health Check;
- 8.3.2 in the event that the IT Health Check report identifies any vulnerabilities, the Supplier shall:
- (a) prepare a remedial plan for approval by the Authority (each a **Remediation Action Plan**) which sets out in respect of each vulnerability identified in the IT Health Check report:
- (i) how the vulnerability will be remedied;
- (ii) unless otherwise agreed in writing between the Parties, the date by which the vulnerability will be remedied, which must be:
- (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 fourteen (14) days 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 fourteen (14) days of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of "Critical";
- (iii) the tests which the Supplier shall perform or procure to be performed (which may, at the discretion of the Authority, include a further IT Health Check) to confirm that the vulnerability has been remedied;
- (b) comply with the Remediation Action Plan; and
- (c) 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.
- 8.4 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 Authority.

- 8.5 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 Authority with a copy of the test report and:
 - 8.5.1 propose interim mitigation measures to vulnerabilities in the Information Management System known to be exploitable where a security patch is not immediately available; and
 - 8.5.2 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 Authority.
- 8.6 The Supplier shall conduct such further tests of the Supplier System as may be reasonably required by the Authority from time to time to demonstrate compliance with its obligations set out in this Schedule and the Contract.
- 8.7 The Supplier shall notify the Authority immediately if it fails to, or believes that it will not, mitigate the vulnerability within the timescales set out in Paragraph 8.3.2.
- 9 Security monitoring and reporting
 - 9.1 The Supplier shall:
 - 9.1.1 monitor the delivery of assurance activities;
 - 9.1.2 maintain and update the Security Management Plan in accordance with Paragraph 6;
 - 9.1.3 agree a document which presents the residual security risks to inform the Authority's decision to give approval to the Supplier to Process and transit the Authority Data;
 - 9.1.4 monitor security risk impacting upon the operation of the Service;
 - 9.1.5 report Breaches of Security in accordance with the approved Incident Management Process; and
 - 9.1.6 agree with the Authority the frequency and nature of the security reports to be prepared and submitted by the Supplier to the Authority within thirty (30) Working Days of Effective Date.
- 10 Malicious Software
 - 10.1 The Supplier shall install and maintain Anti-Malicious Software or procure that Anti-Malicious Software is installed and maintained on any part of the Information Management System which may Process Authority Data and ensure that such Anti-Malicious Software is configured to perform automatic software and definition updates as well as regular scans of the Information Management System to check for, prevent the introduction of Malicious Software or where Malicious Software has been introduced into the Information Management System, to identify, contain the spread of, and minimise the impact of Malicious Software.
 - 10.2 If Malicious Software is found, the parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Authority Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.

- 10.3 Any cost arising out of the actions of the parties taken in compliance with the provisions of Paragraph 10.2 shall be borne by the parties as follows:
- 10.3.1 by the Supplier where the Malicious Software originates from:
- (a) the Supplier Software;
 - (b) the Third Party Software supplied by the Supplier; or
 - (c) the Authority Data whilst the Authority Data is or was under the control of the Supplier,

unless, in the case of the Authority Data only, the Supplier can demonstrate that such Malicious Software was present in the Authority Data and not quarantined or otherwise identified by the Authority when the Authority provided the Authority Data to the Supplier; and
- 10.3.2 by the Authority, in any other circumstance.
- 11 Breach of Security
- 11.1 If either the Authority or the relevant Supplier becomes aware of a Breach of Security it shall notify the other in accordance with the Incident Management Process.
- 11.2 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:
- 11.2.1 Immediately take all reasonable steps necessary to:
- (a) minimise the extent of actual or potential harm caused by such Breach of Security;
 - (b) remedy such Breach of Security to the extent possible;
 - (c) apply a tested mitigation against any such Breach of Security; and
 - (d) prevent a further Breach of Security in the future which exploits the same root cause failure; and
- 11.2.2 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 Authority full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Authority.
- 11.3 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 Sub-contractors 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 Authority.

Appendix A

Security requirements

- 1 Security classification of information
 - 1.1 The Authority shall notify the Supplier of any Authority Data that is OFFICIAL-SENSITIVE, SECRET or TOP SECRET prior to sending or giving the Supplier access to such Authority Data.
 - 1.2 If the provision of the Services requires the Supplier to Process Authority Data which is classified as:
 - 1.2.1 OFFICIAL-SENSITIVE, the Supplier shall implement such additional measures as agreed with the Authority from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards; and/or
 - 1.2.2 SECRET or TOP SECRET, the Supplier shall only do so where it has notified the Authority upon receipt of such Authority Data and the Supplier shall, subject to the Change Control Procedure, implement additional measures as agreed with the Authority 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 Sub-contractors manage, all End-User Devices in accordance with the following requirements:
 - 2.1.1 the operating system and any applications that Process or have access to Authority 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 Authority Data must be encrypted using an encryption tool agreed to by the Authority;
 - 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 Authority Data;
 - 2.1.6 the Supplier or Sub-contractor, as applicable, can, without physical access to the End-User Device, remove or make inaccessible all Authority 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 certification issued by a UKAS-approved certification body, where the scope of that certification includes the Services.
 - 2.2 The Supplier must comply, and ensure that all Sub-contractors 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 Contract.
 - 2.3 Where there any conflict between the requirements of this Schedule 5 (Security Management) and the requirements of the NCSC Device Guidance, the requirements of this Schedule will take precedence.

3 Encryption

3.1 The Supplier must ensure, and must ensure that all Sub-contractors ensure, that Authority 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 Sub-contractor, cannot encrypt Authority Data the Supplier must:

3.2.1 immediately inform the Authority of the subset or subsets of Authority 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 Sub-contractor (as applicable) proposes to take to provide equivalent protection to the Authority as encryption; and

3.2.3 provide the Authority with such information relating to the Authority Data concerned, the reasons why that Authority Data cannot be encrypted and the proposed protective measures as the Authority may require.

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

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

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

3.4.2 the protective measure that the Supplier and/or Sub-contractor will put in place in respect of the unencrypted Authority Data.

3.5 Where the Authority and Supplier do not reach agreement within forty (40) Working Days of the date on which the Supplier first notified the Authority that it could not encrypt certain Authority Data, either Party may refer the matter to be determined in accordance with the Dispute Resolution Procedure.

4 Personnel Security

4.1 All Supplier Personnel 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:

4.1.1 identity;

4.1.2 nationality and immigration status;

4.1.3 employment history; and

4.1.4 criminal record.

4.2 The Authority and the Supplier shall review the roles and responsibilities of the Supplier Personnel who will be involved in the management and/or provision of the Services in order to enable the Authority 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 Authority Data or data which, if it were Authority Data, would be classified as OFFICIAL-SENSITIVE.

- 4.3 The Supplier shall not permit Supplier Personnel 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 Authority 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 Personnel are only granted such access to Authority Data as is necessary to enable the Supplier Personnel to perform their role and to fulfil their responsibilities.
- 4.5 The Supplier shall ensure that Supplier Personnel who no longer require access to the Authority Data (e.g. they cease to be employed by the Supplier or any of its Sub-contractors), have their rights to access the Authority 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 Authority Data receive regular training on security awareness that reflects the degree of access those individuals have to the Sites, the IT Environment or the Authority 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 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 Authority Data (phishing).
- 5 Identity, authentication and access control
 - 5.1 The Supplier shall operate an access control regime to ensure:
 - 5.1.1 all users and administrators of the Supplier System are uniquely identified and authenticated when accessing or administering the Services; and
 - 5.1.2 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 Authority on request.
- 6 Data destruction or deletion
 - 6.1 The Supplier shall:
 - 6.1.1 prior to securely sanitising any Authority Data or when requested the Supplier shall provide the Government with all Authority Data in an agreed open format;
 - 6.1.2 have documented processes to ensure the availability of Authority Data in the event of the Supplier ceasing to trade;
 - 6.1.3 securely erase in a manner agreed with the Authority any or all Authority Data held by the Supplier when requested to do so by the Authority;
 - 6.1.4 securely destroy in a manner agreed with the Authority all media that has held Authority 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 Authority; and
 - 6.1.5 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) 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 Authority Data.
- 7.2 The Supplier and the Authority 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 Authority and documented in the Security Management Plan.

8 Location of Authority Data

The Supplier shall not and shall procure that none of its Sub-contractors Process Authority Data outside the UK without the prior written consent of the Authority, which may be subject to conditions.

9 Vulnerabilities and corrective action

- 9.1 The Authority 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 Authority Data.
- 9.2 The severity of vulnerabilities for COTS Software shall be categorised by the Supplier according to the agreed method in the Security Management Plan and using the appropriate vulnerability scoring systems from the National Vulnerability Database's Vulnerability Severity Ratings (as set out in the CVSS scores at <http://nvd.nist.gov/cvss.cfm>).
- 9.3 Subject to Paragraph 9.4, the Supplier shall procure the application of security patches to vulnerabilities in the Information Management System at all times in accordance with the standard set out within Cyber Essentials Plus as they are updated from time to time.
- 9.4 The timescales for applying patches to vulnerabilities in the Information Management System set out in Paragraph 9.3 shall be extended where:
- 9.4.1 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;
- 9.4.2 the application of a 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 Authority; or
- 9.4.3 the Authority 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 Authority 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:

- 10.1.1 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>;
- 10.1.2 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
- 10.1.3 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:
 - (a) "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;
 - (b) "Cloud Security Principle 2: asset protection and resilience" which, amongst other matters, requires that user data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure;
 - (c) "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;
 - (d) "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;
 - (e) "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;
 - (f) "Cloud Security Principle 6: personnel security" which, amongst other matters, requires that where Supplier Personnel have access to Authority Data and/or the Authority System that those personnel be subject to appropriate security screening and regular security training;
 - (g) "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;
 - (h) "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 Sub-contractors and other suppliers;
 - (i) "Cloud Security Principle 9: secure user management" which, amongst other matters, requires the Supplier to make the tools available for the Authority to securely manage the Authority's use of the Service;
 - (j) "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;
 - (k) "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;

- (l) "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;
- (m) "Cloud Security Principle 13: audit information for users" which, amongst other matters, requires the Supplier to be able to provide the Authority with the audit records it needs to monitor access to the Service and the Authority Data held by the Supplier and/or its Sub-contractors; and
- (n) "Cloud Security Principle 14: secure use of the service" which, amongst other matters, requires the Supplier to educate Supplier Personnel on the safe and secure use of the Information Management System.

Appendix B

Security requirements for Sub-contractors

- 1 Application of Appendix
 - 1.1 This Appendix applies to all Sub-contractors that Process Authority Data.
 - 1.2 The Supplier must:
 - 1.2.1 ensure that those Sub-contractors comply with the provisions of this Appendix;
 - 1.2.2 keep sufficient records to demonstrate that compliance to the Authority; and
 - 1.2.3 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 Sub-contractors to Process Authority Data.
- 2 Designing and managing secure solutions
 - 2.1 The Sub-contractor 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 Sub-contractor must assess their systems against the NCSC Cloud Security Principles:
<https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloud-security/implementing-the-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 Sub-contractor must document that assessment and make that documentation available to the Authority on the Authority's request.
- 3 Data Processing, Storage, Management and Destruction
 - 3.1 The Sub-contractor must not Process any Authority Data outside the UK. The Authority may permit the Sub-contractor to Process Authority Data outside the UK and may impose conditions on that permission, with which the Sub-contractor must comply. Any permission must be in writing to be effective.
 - 3.2 The Sub-contractor must when requested to do so by the Authority:
 - 3.2.1 securely destroy Authority Data only on Sites which are included within the scope of an existing certification of compliance with ISO/IEC 27001;
 - 3.2.2 satisfy the Authority that their data destruction/deletion practices comply with UK GDPR requirements and follows all relevant NCSC guidance; and
 - 3.2.3 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 Sub-contractor 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:
 - 4.1.1 identity;
 - 4.1.2 nationality and immigration status;
 - 4.1.3 employment history; and

4.1.4 criminal record.

The HMG Baseline Personnel Security Standard is at <https://www.gov.uk/government/publications/government-baseline-personnel-security-standard>.

4.2 The Sub-contractor must, if the Authority requires, at any time, ensure that one or more of the Sub-contractor's staff obtains Security Check clearance in order to Process Authority Data containing Personal Data above certain volumes specified by the Authority, or containing Special Category Personal Data.

4.3 Any Sub-contractor 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 Sub-contractors manage, all End-User Devices used by the Supplier in accordance with the following requirements:

5.1.1 the operating system and any applications that Process or have access to Authority Data must be in current support by the vendor, or the relevant community in the case of Open Source operating systems or applications;

5.1.2 users must authenticate before gaining access;

5.1.3 all Authority Data must be encrypted using an encryption tool agreed to by the Authority;

5.1.4 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;

5.1.5 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 Authority Data;

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

5.1.7 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 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 Sub-contractors 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 Contract.

5.3 Where there any conflict between the requirements of this Schedule 5 (Security Management) and the requirements of the NCSC Device Guidance, the requirements of this Schedule will take precedence.

6 Encryption

6.1 The Supplier must ensure, and must ensure that all Sub-contractors ensure, that Authority Data is encrypted:

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

6.1.2 when transmitted.

- 6.2 Where the Supplier, or a Sub-contractor, cannot encrypt Authority Data the Supplier must:
- 6.2.1 immediately inform the Authority of the subset or subsets of Authority Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;
 - 6.2.2 provide details of the protective measures the Supplier or Sub-contractor (as applicable) proposes to take to provide equivalent protection to the Authority as encryption; and
 - 6.2.3 provide the Authority with such information relating to the Authority Data concerned, the reasons why that Authority Data cannot be encrypted and the proposed protective measures as the Authority may require.
- 6.3 The Authority, the Supplier and, where the Authority requires, any relevant Sub-contractor shall meet to agree appropriate protective measures for the unencrypted Authority Data.
- 6.4 Where the Authority and Supplier reach agreement, the Supplier must update the Security Management Plan to include:
- 6.4.1 the subset or subsets of Authority Data not encrypted and the circumstances in which that will occur; and
 - 6.4.2 the protective measure that the Supplier and/or Sub-contractor will put in place in respect of the unencrypted Authority Data.
- 6.5 Where the Authority and Supplier do not reach agreement within forty (40) Working Days of the date on which the Supplier first notified the Authority that it could not encrypt certain Authority Data, either Party may refer the matter to be determined in accordance with the Dispute Resolution Procedure.
- 7 Patching and vulnerability scanning
- The Sub-contractor 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 Sub-contractors
- 8.1 The Sub-contractor must not transmit or disseminate the Authority Data to any other person unless specifically authorised by the Authority. Such authorisation must be in writing to be effective and may be subject to conditions.
 - 8.2 The Sub-contractor must not, when performing any part of the Services, use any software to Process the Authority Data where the licence terms of that software purport to grant the licensor rights to Process the Authority Data greater than those rights strictly necessary for the use of the software.

Appendix C

Security Management Plan Template for Part 1 and Part 2

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 these should be noted. Any off-shoring considerations should be detailed.)
 - 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 2 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.]

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 alter bank details.	Medium – high	Users bank details can be altered as part of the normal business function.	C12. System administrators hold SC clearance. 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	Low

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.
C15	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 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

4.1 [●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 certification should be included. This section should include at least:

- 4.1.1 information risk management and timescales and triggers for a review;
- 4.1.2 contractual patching requirements and timescales for the different priorities of patch;
- 4.1.3 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;
- 4.1.4 configuration and change management;
- 4.1.5 incident management;
- 4.1.6 vulnerability management;
- 4.1.7 user access management; and
- 4.1.8 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

[●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 Authority/Customer, should be included here. It must as a minimum include the protocol for how and when incidents will be reported to the Authority/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 November 2018	July 2019	Open

10 Sub-contractors

[●This should include a table which shows for each Sub-contractor 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 and/or Cyber Essential Plus certificates

[●Any certifications relied upon should have their certificates included.]

12 Annex B. Cloud Security Principles assessment

[●A spreadsheet may be attached.]

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

[●A spreadsheet may be attached.]

14 Annex D. Latest ITHC report and Remediation Action Plan

Part 2: Security Accreditation

1 Application

Part 2 (Security Accreditation) of this Schedule 5 shall only apply to the Implementation Services as is supplied by Supplier B or (where expressly stated in the Contract) Supplier A.

2 Definitions

2.1 In this Schedule, the definitions in Schedule 1 (Definitions) shall apply.

3 Introduction

3.1 This Part 2 of this Schedule sets out:

- 3.1.1 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 Authority Data, the IT Environment, the Services and the Information Management System;
- 3.1.2 the process which shall apply to the Accreditation of the Core Information Management System in Paragraph 7;
- 3.1.3 the Certification Requirements applicable to the Wider Information Management System in Paragraph 8;
- 3.1.4 the Security Tests which the Supplier shall conduct during the Contract Period in Paragraph 9;
- 3.1.5 the Security Tests which the Authority may conduct during the Contract Period in Paragraph 9.6;
- 3.1.6 the requirements to patch vulnerabilities in the Core Information Management System in Paragraph 10;
- 3.1.7 the obligations on the Supplier to prevent the introduction of Malicious Software into the Information Management System and to scan for, contain the spread of, and minimise the impact of Malicious Software which is introduced into the Information Management System in Paragraph 11; and
- 3.1.8 each Party's obligations in the event of an actual or attempted Breach of Security in Paragraph 12.

4 Principles of Security

4.1 Each Supplier acknowledges that the Authority places great emphasis on the confidentiality, integrity and availability of the Authority Data and, consequently on the security of:

- 4.1.1 the Sites;
- 4.1.2 the IT Environment;
- 4.1.3 the Services; and
- 4.1.4 the Core Information Management System.

4.2 Notwithstanding the involvement of the Authority in the Accreditation of the Core Information Management System, the Supplier shall be and shall remain responsible for:

- 4.2.1 the security, confidentiality, integrity and availability of the Authority Data whilst that Authority Data is under the control of the Supplier or any of its Sub-contractors; and

- 4.2.2 the security of the Information Management System.
- 4.3 Each Supplier shall:
 - 4.3.1 comply with the Baseline Security Requirements; and
 - 4.3.2 ensure that each Sub-contractor that Processes Authority Data complies with the Sub-contractor Security Requirements.
- 4.4 The Service Management Board established under Schedule 21 (Governance) shall, in addition to its responsibilities set out in that Schedule, monitor and may also provide recommendations to the Supplier on the Accreditation of the Core Information Management System.
- 4.5 To facilitate the Supplier's design, implementation, operation, management and continual improvement of the Security Management Plan and the security of the Services and Information Management System and otherwise:
 - 4.5.1 the Supplier shall provide access to the Supplier Personnel responsible for information assurance; and
 - 4.5.2 the Authority shall provide access to its personnel responsible for information assurance,in each case at reasonable times on reasonable notice.
- 5 Information Management System
 - 5.1 The Information Management System comprises the Core Information Management System and the Wider Information Management System.
 - 5.2 The component parts of the Core Information Management System and its boundary with the Wider Information Management System are shown in the diagram in Appendix C of Part 2 of this Schedule.
 - 5.3 Any proposed change to the component parts of the Core Information Management System or the boundary between the Core Information Management System and the Wider Information Management System shall be notified and processed in accordance with the Change Control Procedure.
- 6 Statement of Information Risk Appetite and Baseline Security Requirements
 - 6.1 Each Supplier acknowledges that the Authority has provided and the Supplier has received a statement of information risk appetite for the Supplier System and the Services (the **Statement of Information Risk Appetite**).
 - 6.2 The Authority's Baseline Security Requirements in respect of the Core Information Management System are set out in Appendix A of Part 2 of this Schedule.
- 7 Accreditation of the Core Information Management System
 - 7.1 The Core Information Management System shall be subject to Accreditation in accordance with this Paragraph 7.
 - 7.2 Each Supplier acknowledges that the purpose of Accreditation is to ensure that:
 - 7.2.1 the Security Management Plan accurately represents the Core Information Management System;
 - 7.2.2 the Accreditation Plan, if followed, provides the Authority with sufficient confidence that the CIMS will meet the requirements of the Baseline Security Requirements and the Statement of Risk Appetite; and

- 7.2.3 the residual risks of the Core Information Management System are no greater than those provided for in the Statement of Risk Appetite and Baseline Security Requirements.
- 7.3 The Accreditation shall be performed by the Authority or by representatives appointed by the Authority.
- 7.4 In addition to any obligations imposed by Schedule 13 (Implementation Plan) or Schedule 14 (Testing Procedures) the Supplier must ensure that its Detailed Implementation Plan sets out in sufficient detail how it will ensure compliance with the requirements of this Schedule 5 (Security Management), including any requirements imposed on Sub-contractors by Appendix B of Part 2 of this Schedule, from any relevant Operational Service Commencement Date.
- 7.5 By the date specified in the Detailed Implementation Plan, the Supplier shall prepare and submit to the Authority the risk management documentation for the Core Information Management System, which shall be subject to approval by the Authority in accordance with, this Paragraph 7 (the **Security Management Plan**).
- 7.6 The Security Management Plan shall be structured in accordance with the template as set out in Appendix C of Part 1 and include:
- 7.6.1 the Accreditation Plan, which shall include:
- (a) the dates on which each subsequent iteration of the Security Management Plan will be delivered to the Authority for review and staged approval; and
- (b) the date by which the Supplier is required to have received a Residual Risk Statement from the Authority together with details of each of the tasks which must be completed by the Supplier, Milestones which must be Achieved and the Authority Responsibilities which must be completed in order for the Supplier to receive a Residual Risk Statement pursuant to Paragraph 7.11;
- 7.6.2 a formal risk assessment of the Core Information Management System and a risk treatment plan for the Core Information Management System;
- 7.6.3 a completed ISO/IEC 27001 Statement of Applicability for the Core Information Management System; the process for managing any security risks from Sub-contractors and third parties authorised by the Authority with access to the Services, processes associated with the delivery of the Services, the Authority Premises, the Sites, the Supplier System, the Authority System (to extent that it is under the control of the Supplier) and any IT, Information and data (including the Confidential Information of the Authority and the Authority Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Services;
- 7.6.4 unless such requirement is waived by the Authority, proposed controls that will be implemented in respect of all aspects of the Services and all processes associated with the delivery of the Services, including the Authority Premises, the Sites, the Supplier System, the Authority System (to the extent that it is under the control of the Supplier) and any IT, Information and data (including the Confidential Information of the Authority and the Authority Data) to the extent used by the Authority or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Services;
- 7.6.5 the Required Changes Register;
- 7.6.6 evidence that the Supplier and each applicable Sub-contractor is compliant with the Certification Requirements; and

- 7.6.7 the diagram documenting the Core Information Management System, the Wider Information Management System and the boundary between them contained in Appendix C of Part 2 of this Schedule.
- 7.7 To facilitate Accreditation of the Core Information Management System, the Supplier shall provide the Authority and its authorised representatives with:
 - 7.7.1 access to the Sites, ICT information assets and ICT systems within the Core Information Management System on request or in accordance with the Accreditation Plan; and
 - 7.7.2 such other information and/or documentation that the Authority or its authorised representatives may reasonably require, to enable the Authority to establish that the Core Information Management System is compliant with the Security Management Plan.
- 7.8 The Authority shall, by the relevant date set out in the Accreditation Plan, review the Security Management Plan and issue to the Supplier either:
 - 7.8.1 a Residual Risk Statement which will then form part of the Security Management Plan, confirming that the Authority is satisfied that the identified risks to the Core Information Management System have been adequately and appropriately addressed and that the residual risks are understood and accepted by the Authority; or
 - 7.8.2 a rejection notice stating that the Authority considers that the identified risks to the Core Information Management System have not been adequately or appropriately addressed, or the residual risks to the Core Information Management System have not been reduced to the level anticipated by the Statement of Information Risk Appetite, and the reasons why (**Risk Management Rejection Notice**).
- 7.9 If the Authority issues a Risk Management Rejection Notice, the Supplier shall, within twenty (20) Working Days of the date of the Risk Management Rejection Notice:
 - 7.9.1 address all of the issues raised by the Authority in such notice;
 - 7.9.2 update the Security Management Plan, as appropriate, and
 - 7.9.3 notify the Authority that the Core Information Management System is ready for an Accreditation Decision.
- 7.10 If the Authority issues two or more Risk Management Rejection Notices, the failure to receive a Residual Risk Statement shall constitute a material Default and the Authority may by terminate this Contract with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 31.1.2.
- 7.11 Subject to Paragraph 7.10, the process set out in Paragraphs 7.8 to 7.10 shall be repeated until such time as the Authority issues a Residual Risk Statement to the Supplier or terminates this Contract.
- 7.12 Each Supplier shall not use the Core Information Management System to Process Authority Data before receiving a Residual Risk Statement.
- 7.13 Each Supplier shall keep the Core Information Management System and Security Management Plan under review and shall update the Security Management Plan annually in accordance with this Paragraph and the Authority shall review the Accreditation Decision annually and following the occurrence of any of the events set out in Paragraph 7.15.
- 7.14 Each Supplier shall notify the Authority within two (2) Working Days after becoming aware of:
 - 7.14.1 a significant change, or a significant planned change, to the components or architecture of the Core Information Management System;

- 7.14.2 a new risk or vulnerability is identified to the components or architecture of the Core Information Management System;
 - 7.14.3 a change in the threat profile;
 - 7.14.4 a Sub-contractor failure to comply with the Core Information Management System code of connection;
 - 7.14.5 a significant change to any risk component;
 - 7.14.6 a significant change in the quantity of Personal Data held within the Core Information Management System;
 - 7.14.7 where the Supplier has previously Processed Personal Data that does not include Special Category Personal Data, it starts to, or proposes to start to, Process Special Category Personal Data under this Contract;
 - 7.14.8 a proposal to change any of the Sites from which any part of the Services are provided; and/or
 - 7.14.9 an ISO/IEC 27001 audit report produced in connection with the Certification Requirements indicates significant concerns; and
 - 7.14.10 update the Required Changes Register and provide the updated Required Changes Register to the Authority for review and approval within ten (10) Working Days after the initial notification or such other timescale as may be agreed with the Authority.
- 7.15 If the Supplier fails to implement a change set out in the Required Changes Register by the date agreed with the Authority, such failure shall constitute a material Default and the Supplier shall:
- 7.15.1 immediately cease using the Core Information Management System to Process Authority Data until the Default is remedied, unless directed otherwise by the Authority in writing and then it may only continue to Process Authority Data in accordance with the Authority's written directions; and
 - 7.15.2 where such Default is capable of remedy, the Supplier shall remedy such Default within the timescales set by the Authority and, should the Supplier fail to remedy the Default within such timescales, the Authority may terminate this Contract with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 31.1.2.
- 7.16 Each Supplier shall review each Change Request against the Security Management Plan to establish whether the documentation would need to be amended should such Change Request be agreed and, where a Change Request would require an amendment to the Security Management Plan, the Supplier shall set out any proposed amendments to the documentation in the Impact Assessment associated with such Change Request for consideration and approval by the Authority.
- 7.17 Each Supplier shall be solely responsible for the costs associated with developing and updating the Security Management Plan and carrying out any remedial action required by the Authority as part of the Accreditation process.
- 8 Certification Requirements
- 8.1 Each Supplier shall ensure, at all times during the Term, that it is certified as compliant with:
- 8.1.1 ISO/IEC 27001 by a UK Accreditation Service (UKAS)-approved certification body or are included within the scope of an existing certification of compliance with ISO/IEC 27001; and
 - 8.1.2 Cyber Essentials Plus,

and shall provide the Authority with a copy of each such certificate of compliance before the Supplier shall be permitted to use the Core Information Management System to receive or Process Authority Data.

- 8.2 Notwithstanding anything else in this Contract, a CIMS Sub-contractor shall be treated for all purposes as a Key Sub-contractor.
- 8.3 In addition to the obligations contained in Clause 15 (Appointment of Sub-contractors), the Supplier must ensure that the Key Sub-contract with each CIMS Sub-contractor:
 - 8.3.1 contains obligations no less onerous on the Key Sub-contractor than those imposed on the Supplier under this Schedule 5 (Security Management); but
 - 8.3.2 provides for the Authority to perform Accreditation of any part of the Core Information Management System that the CIMS Sub-contractor provides or operates which is not otherwise subject to Accreditation under this Schedule 5 (Security Management).
- 8.4 Each Supplier shall ensure that each Higher Risk Sub-contractor is certified as compliant with either:
 - 8.4.1 ISO/IEC 27001 by a UK Accreditation Service (UKAS)-approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001; or
 - 8.4.2 Cyber Essentials Plus,and shall provide the Authority with a copy of each such certificate of compliance before the Higher-Risk Sub-contractor shall be permitted to receive or Process Authority Data.
- 8.5 Each Supplier shall ensure that each Sub-contractor is certified compliant with Cyber Essentials.
- 8.6 Each Supplier shall ensure that the Supplier and each Sub-contractor who is responsible for the secure destruction of Authority Data:
 - 8.6.1 securely destroys Authority Data only on Sites which are included within the scope of an existing certification of compliance with ISO/IEC 27001;
 - 8.6.2 should satisfy the Authority that their data destruction/deletion practices comply with UK GDPR requirements and follows all relevant NCSC guidance; and
 - 8.6.3 must maintain an asset register of all Authority supplied information, data and equipment to ensure Authority assets are returned and/or deleted.
- 8.7 Each Supplier shall provide the Authority with evidence of its and its Sub-contractor's compliance with the requirements set out in this Paragraph before the Supplier or the relevant Sub-contractor (as applicable) shall be permitted to carry out the secure destruction of the Authority Data.
- 8.8 Each Supplier shall notify the Authority as soon as reasonably practicable and, in any event within two (2) Working Days, if the relevant Supplier or any Sub-contractor ceases to be compliant with the Certification Requirements and shall or shall procure that the relevant Sub-contractor shall:
 - 8.8.1 immediately ceases receiving or Processing Authority Data; and
 - 8.8.2 procure that the relevant Sub-contractor promptly returns, destroys and/or erases the Authority Data in accordance with Baseline Security Requirements.
- 8.9 The Authority may agree to exempt in whole or part the relevant Supplier or any Sub-contractor from the Certification Requirements. Any exemption must be in writing to be effective. Each Supplier must include the exemption in the Security Management Plan.

- 9 Security Testing
- 9.1 Each Supplier shall, at its own cost and expense:
- 9.1.1 procure testing of the Core Information Management System by a CHECK Service Provider or a CREST Service Provider (an **IT Health Check**):
 - (a) prior to it submitting the Security Management Plan to the Authority for an Accreditation Decision;
 - (b) before the relevant Supplier is given permission by the Authority to Process or manage any Authority Data;
 - (c) if directed to do so by the Authority; and
 - (d) once every twelve (12) months during the Term;
 - 9.1.2 conduct vulnerability scanning and assessments of the Core Information Management System monthly;
 - 9.1.3 conduct an assessment as soon as reasonably practicable following receipt by the relevant Supplier or any of its Sub-contractors of a "Critical" or "High" vulnerability alert from a supplier of any software or other component of the Core Information Management System to determine whether the vulnerability affects the Core Information Management System; and
 - 9.1.4 conduct such other tests as are required by:
 - (a) any Remediation Action Plans;
 - (b) the ISO/IEC 27001 certification requirements;
 - (c) the Security Management Plan; and
 - (d) the Authority following a Breach of Security or a significant change to the components or architecture of the Core Information Management System,(each a **Security Test**).
- 9.2 The Supplier shall provide the Authority with the results of such Security Tests (in a form approved by the Authority in advance) as soon as practicable, and in any case within ten (10) Working Days, after completion of each Security Test.
- 9.3 In relation to each IT Health Check, the Supplier shall:
- 9.3.1 agree with the Authority the aim and scope of the IT Health Check;
 - 9.3.2 promptly, and in any case no later than ten (10) Working Days, following receipt of each IT Health Check report, provide the Authority with a copy of the IT Health Check report;
 - 9.3.3 in the event that the IT Health Check report identifies any vulnerabilities, the Supplier shall:
 - (a) prepare a remedial plan for approval by the Authority (each a **Remediation Action Plan**) which sets out in respect of each vulnerability identified in the IT Health Check report:
 - (i) how the vulnerability will be remedied;

- (ii) unless otherwise agreed in writing between the Parties, the date by which the vulnerability will be remedied, which must be:
 - (1) within three (3) months of the date the relevant 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 relevant 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 relevant Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of "critical";
 - (iii) the tests which the relevant Supplier shall perform or procure to be performed (which may, at the discretion of the Authority, include a further IT Health Check) to confirm that the vulnerability has been remedied;
 - (b) comply with the Remediation Action Plan; and
 - (c) conduct such further Security Tests on the Core Information Management System to provide independent evidence that the relevant Supplier has complied with the Remediation Action Plan.
- 9.4 The Security Tests 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 Security Tests shall be agreed in advance with the Authority. Subject to the Supplier complying with this Paragraph 9.4, if a Security Test causes a Performance Failure in a particular Measurement Period, the Supplier shall be granted relief in respect of such Performance Failure for that Measurement Period.
- 9.5 The Authority shall be entitled to send a representative to witness the conduct of the Security Tests. Without prejudice to the Supplier's obligations under Paragraph 9.3, the Supplier shall provide the Authority with the results of such Security Tests (in a form approved by the Authority in advance) as soon as practicable, and in any case no later than ten (10) Working Days, after completion of each Security Test.
- 9.6 The Authority and/or its authorised representatives shall be entitled, at any time and without giving notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the Service, the Information Management System and/or the Supplier's compliance with the Security Management Plan (**Authority Security Tests**). The Authority shall take reasonable steps to notify the relevant Supplier prior to carrying out such Authority Security Test to the extent that it is reasonably practicable for it to do so taking into account the nature of the Authority Security Test.
- 9.7 The Authority shall notify the relevant Supplier of the results of such Authority Security Tests after completion of each Authority Security Test.
- 9.8 The Authority Security Tests shall be designed and implemented so as to minimise their impact on the delivery of the Services. If an Authority Security Test causes Supplier Non-Performance, the Authority Security Test shall be treated as an Authority Cause, except where the root cause of the relevant Supplier Non-Performance was a weakness or vulnerability exposed by the Authority Security Test.
- 9.9 Without prejudice to the provisions of Paragraph 9.3.3, where any Security Test carried out pursuant to this Paragraph 9 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the relevant Supplier shall promptly notify the Authority of any changes to the Core Information Management System and/or the Security Management Plan (and the implementation thereof) which relevant Supplier proposes to make in order to correct such failure or weakness. Subject to the Authority's prior written approval, the relevant Supplier

shall implement such changes to the Core Information Management System and/or the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Authority or, otherwise, as soon as reasonably possible.

- 9.10 If the Authority unreasonably withholds its approval to the implementation of any changes proposed by the relevant Supplier to the Security Management Plan in accordance with Paragraph 9.9 above, the relevant Supplier shall not be deemed to be in breach of this Contract to the extent it can be shown that such breach:
- 9.10.1 has arisen as a direct result of the Authority unreasonably withholding its approval to the implementation of such proposed changes; and
 - 9.10.2 would have been avoided had the Authority given its approval to the implementation of such proposed changes.
- 9.11 For the avoidance of doubt, where a change to the Core Information Management System and/or the Security Management Plan is required to remedy non-compliance with the Risk Management Documentation, the Baseline Security Requirements and/or any obligation in this Contract, the Supplier shall effect such change at its own cost and expense.
- 9.12 If any repeat Security Test carried out pursuant to Paragraph 9.9 reveals an actual or potential Breach of Security or weakness exploiting the same root cause failure, such circumstance shall constitute a material Default and the Authority may by terminate this Contract with immediate effect by issuing a Termination Notice to the relevant Supplier in accordance with Clause 31.1.2.
- 9.13 Each Supplier shall, by the expiry of each Contract Year provide to the Authority a letter from its chief executive officer (or equivalent officer) confirming that having made due and careful enquiry:
- 9.13.1 the Supplier has in the previous year carried out all tests and has in place all procedures required in relation to security matters under this Contract; and
 - 9.13.2 the Supplier is confident that its security and risk mitigation procedures with respect to the Services remain effective.
- 10 Vulnerabilities and corrective action
- 10.1 The Authority 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 Authority Data.
- 10.2 The severity of vulnerabilities for COTS Software shall be categorised by the Supplier according to the agreed method in the Security Management Plan and using the appropriate vulnerability scoring systems from the National Vulnerability Database's Vulnerability Severity Ratings (as set out in the CVSS scores at <http://nvd.nist.gov/cvss.cfm>).
- 10.3 Subject to Paragraph 10.4, the Supplier shall procure the application of security patches to vulnerabilities in the Core Information Management System in accordance with the standards set out within Cyber Essentials Plus as they are updated from time to time.
- 10.4 The timescales for applying patches to vulnerabilities in the Core Information Management System set out in Paragraph 10.3 shall be extended where:
- 10.4.1 the relevant Supplier can demonstrate that a vulnerability in the Core 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 relevant Supplier within the timescales set out in Paragraph 10.3 if the vulnerability becomes exploitable within the context of the Services;

- 10.4.2 the application of a security patch adversely affects the Supplier's ability to deliver the Services in which case the relevant Supplier shall be granted an extension to such timescales of five (5) days, provided the relevant Supplier had followed and continues to follow the security patch test plan agreed with the Authority; or
- 10.4.3 the Authority agrees a different maximum period after a case-by-case consultation with the relevant Supplier under the processes defined in the Security Management Plan.
- 10.5 The Security Management Plan shall include provisions for major version upgrades of all Supplier COTS Software and Third Party COTS Software to be kept up to date such that all Supplier COTS Software and Third Party COTS Software are always with support throughout the Term unless otherwise agreed by the Authority in writing.
- 10.6 Each Supplier shall:
 - 10.6.1 implement a mechanism for receiving, analysing and acting upon threat information supplied by NCSC, or any other competent Central Government Body;
 - 10.6.2 promptly notify NCSC of any actual or sustained attempted Breach of Security;
 - 10.6.3 ensure that the Core Information Management System is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;
 - 10.6.4 ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the Core Information Management System by actively monitoring the threat landscape during the Term;
 - 10.6.5 pro-actively scan the Core Information Management System for vulnerable components and address discovered vulnerabilities through the processes described in the Security Management Plan;
 - 10.6.6 from the date specified in the Accreditation Plan and within five (5) Working Days of the end of each subsequent month during the Term, provide the Authority with a written report which details both patched and outstanding vulnerabilities in the Core Information Management System, the elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report and any failure to comply with the timescales set out in Paragraph 10.3 for applying patches to vulnerabilities in the Core Information Management System;
 - 10.6.7 propose interim mitigation measures to vulnerabilities in the Core Information Management System known to be exploitable where a security patch is not immediately available;
 - 10.6.8 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 Core Information Management System); and
 - 10.6.9 inform the Authority when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the Core Information Management System and provide initial indications of possible mitigations.
- 10.7 If either Supplier is unlikely to be able to mitigate the vulnerability within the timescales under Paragraph 10.3, the relevant Supplier shall immediately notify the Authority.
- 10.8 If either Supplier fails to patch vulnerabilities in the Core Information Management System in accordance with Paragraph 10.3, such failure shall constitute a material Default and the

Authority may by terminate this Contract with immediate effect by issuing a Termination Notice to the relevant Supplier.

11 Malicious Software

11.1 Each Supplier shall install and maintain Anti-Malicious Software or procure that Anti-Malicious Software is installed and maintained on any part of the Information Management System which may Process Authority Data and ensure that such Anti-Malicious Software is configured to perform automatic software and definition updates as well as regular scans of the Information Management System to check for, prevent the introduction of Malicious Software or where Malicious Software has been introduced into the Information Management System, to identify, contain the spread of, and minimise the impact of Malicious Software.

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

11.3 Any cost arising out of the actions of the Parties taken in compliance with the provisions of Paragraph 11.2 shall be borne by the Parties as follows:

11.3.1 by the relevant Supplier where the Malicious Software originates from:

- (a) the relevant Supplier's Software;
- (b) the Third-Party Software supplied by the relevant Supplier; or
- (c) the Authority Data whilst the Authority Data is or was under the control of the relevant Supplier,

unless, in the case of the Authority Data, the relevant Supplier can demonstrate that such Malicious Software was present in the Authority Data and not quarantined or otherwise identified by the Authority when the Authority provided the Authority Data to the relevant Supplier; and

11.3.2 otherwise by the Authority.

12 Breach of Security

12.1 If either the Authority or the relevant Supplier becomes aware of a Breach of Security or an attempted Breach of Security it shall notify the other in accordance with the security incident management process as set out in the Security Management Plan.

12.2 The security incident management process set out in the Security Management Plan shall, as a minimum, require the Supplier upon becoming aware of a Breach of Security or an attempted Breach of Security to:

12.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Authority which shall be completed within such timescales as the Authority may reasonably require) necessary to:

- (a) minimise the extent of actual or potential harm caused by such Breach of Security;
- (b) remedy such Breach of Security to the extent possible and protect the integrity of the Information Management System against any such potential or attempted Breach of Security;
- (c) apply a tested mitigation against any such Breach of Security or potential or attempted Breach of Security and, provided that reasonable testing has been undertaken by the relevant Supplier, if the mitigation adversely affects the Supplier's ability to deliver the Services so as to meet any Performance Indicator, the relevant Supplier shall be granted relief against the failure to meet such

affected Performance Indicator for such period as the Authority, acting reasonably, may specify by written notice to the relevant Supplier; and

- (d) prevent a further Breach of Security or attempted Breach of Security in the future exploiting the same root cause failure; and

12.2.2 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 Authority full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Authority.

12.3 In the event that any action is taken in response to a Breach of Security or attempted Breach of Security which occurred as a result of non-compliance of the Information Management System and/or the Security Management Plan with the Baseline Security Requirements and/or this Contract, then such action and any required change to the Information Management System and/or Security Management Plan shall be completed by the relevant Supplier at no cost to the Authority.

12.4 If either Supplier fails to comply with its obligations set out in this Paragraph 12, such failure shall constitute a material Default, which if not remedied to the satisfaction of the Authority, shall permit the Authority to terminate this Contract with immediate effect by issuing a Termination Notice to the relevant Supplier.

13 Data Processing, Storage, Management and Destruction

13.1 In addition to the obligations on the Supplier set out Clause 21 (Protection of Personal Data) in respect of Processing Personal Data and compliance with the Data Protection Legislation, the Supplier shall:

13.1.1 Process Authority Data only in the UK, except where the Authority has given its consent in writing to a transfer of the Authority Data to such other country;

13.1.2 on demand, provide the Authority with all Authority Data in an agreed open format;

13.1.3 have documented processes to guarantee availability of Authority Data in the event of the relevant Supplier ceasing to trade;

13.1.4 securely erase any or all Authority Data held by the relevant Supplier when requested to do so by the Authority; and

13.1.5 securely destroy all media that has held Authority 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 directed by the Authority.

Appendix A

Baseline Security Requirements

- 1 Security classification of information
 - 1.1 The Authority shall notify the Supplier of any Authority Data that is OFFICIAL-SENSITIVE, SECRET or TOP SECRET prior to sending or giving the Supplier access to such Authority Data.
 - 1.2 If the provision of the Services requires either Supplier to Process Authority Data which is classified as:
 - 1.2.1 OFFICIAL-SENSITIVE, the relevant Supplier shall implement such additional measures as agreed with the Authority from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards; and/or
 - 1.2.2 SECRET or TOP SECRET, the relevant Supplier shall only do so where it has notified the Authority upon receipt of such Authority Data and the relevant Supplier shall, subject to the Change Control Procedure, implement additional measures as agreed with the Authority 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 Each Supplier must manage, and must ensure that all Sub-contractors manage, all End-User Devices used by the relevant Supplier in accordance with the following requirements:
 - 2.1.1 the operating system and any applications that Process or have access to Authority 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 Authority Data must be encrypted using an encryption tool agreed to by the Authority;
 - 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 Authority Data;
 - 2.1.6 the Supplier or Sub-contractor, as applicable, can, without physical access to the End-User Device, remove or make inaccessible all Authority 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 relevant Supplier, or any ISO/IEC 27001 certification issued by a UKAS-approved certification body, where the scope of that certification includes the Services.
 - 2.2 Each Supplier must comply, and ensure that all Sub-contractors 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 Contract.

- 2.3 Where there any conflict between the requirements of this Schedule 5 (Security Management) and the requirements of the NCSC Device Guidance, the requirements of this Schedule will take precedence.
- 3 Encryption
- 3.1 Each Supplier must ensure, and must ensure that all Sub-contractors ensure, that Authority 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 either Supplier, or a Sub-contractor, cannot encrypt Authority Data the relevant Supplier must:
- 3.2.1 immediately inform the Authority of the subset or subsets of Authority 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 relevant Supplier or Sub-contractor (as applicable) proposes to take to provide equivalent protection to the Authority as encryption; and
- 3.2.3 provide the Authority with such information relating to the Authority Data concerned, the reasons why that Authority Data cannot be encrypted and the proposed protective measures as the Authority may require.
- 3.3 The Authority, the relevant Supplier and, where the Authority requires, any relevant Sub-contractor shall meet to agree appropriate protective measures for the unencrypted Authority Data.
- 3.4 Where the Authority and Supplier reach agreement, the Supplier must update the Security Management Plan to include:
- 3.4.1 the subset or subsets of Authority Data not encrypted and the circumstances in which that will occur; and
- 3.4.2 the protective measure that the relevant Supplier and/or Sub-contractor will put in place in respect of the unencrypted Authority Data.
- 3.5 Where the Authority and Supplier do not reach agreement within forty (40) Working Days of the date on which the relevant Supplier first notified the Authority that it could not encrypt certain Authority Data, either Party may refer the matter to be determined in accordance with the Dispute Resolution Procedure.
- 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.
- 4.2 The Authority and the Supplier shall review the roles and responsibilities of the relevant Supplier's Staff who will be involved in the management and/or provision of the Services in order to enable the Authority 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 Authority Data or data which, if it were Authority Data, would be classified as OFFICIAL-SENSITIVE.

- 4.3 Each 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 Authority has expressly agreed in writing to the involvement of the named individual in the management and/or provision of the Services.
- 4.4 Each Supplier shall ensure that the relevant Supplier's Staff are only granted such access to Authority Data as is necessary to enable the relevant Supplier's Staff to perform their role and to fulfil their responsibilities.
- 4.5 Each Supplier shall ensure that Supplier Staff who no longer require access to the Authority Data (e.g. they cease to be employed by the relevant Supplier or any of its Sub-contractors), have their rights to access the Authority Data revoked within one (1) Working Day.
- 4.6 Each Supplier shall ensure that Supplier Staff that have access to the Sites, the IT Environment or the Authority Data receive regular training on security awareness that reflects the degree of access those individuals have to the Sites, the IT Environment or the Authority Data.
- 4.7 Each 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 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 Authority Data (phishing).
- 5 Identity, authentication and access control
 - 5.1 Each Supplier shall operate an access control regime to ensure:
 - 5.1.1 all users and administrators of the relevant Supplier's Supplier System are uniquely identified and authenticated when accessing or administering the Services; and
 - 5.1.2 all persons who access the Sites are identified and authenticated before they are allowed access to the Sites.
 - 5.2 Each Supplier shall apply the "principle of least privilege" when allowing persons access to that Supplier's Supplier System and Sites so that such persons are allowed access only to those parts of the Sites and the relevant Supplier's Supplier System that they require.
 - 5.3 Each Supplier shall retain records of access to the Sites and to its Supplier System and shall make such record available to the Authority on request.
- 6 Audit and protective monitoring
 - 6.1 Each Supplier shall collect audit records which relate to security events in Core 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) include regular reports and alerts setting out details of access by users of the Core 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 Authority Data.
 - 6.2 In addition to any requirement in Clause 37.3, Each Supplier shall:
 - 6.2.1 implement audit and monitoring of the Core Information Management System sufficient to comply with any applicable Relevant Requirements and to prevent or detect any Prohibited Act;

- 6.2.2 keep sufficient records to demonstrate compliance with the requirements of Paragraph 6.2.1 to the Authority; and
- 6.2.3 make those records and any documents describing the audit and monitoring undertaken to the Authority on request.
- 6.3 Each Supplier and the Authority shall work together to establish any additional audit and monitoring requirements for the Core Information Management System.
- 6.4 The retention periods for audit records and event logs must be agreed with the Authority and documented in the Security Management Plan.
- 7 Secure architecture
- 7.1 Each Supplier shall design the Core Information Management System in accordance with:
 - 7.1.1 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>;
 - 7.1.2 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
 - 7.1.3 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:
 - (a) "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;
 - (b) "Cloud Security Principle 2: asset protection and resilience" which, amongst other matters, requires that user data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure;
 - (c) "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;
 - (d) "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;
 - (e) "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;
 - (f) "Cloud Security Principle 6: personnel security" which, amongst other matters, requires that where Supplier Staff have access to Authority Data and/or the Authority System that those personnel be subject to appropriate security screening and regular security training;
 - (g) "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;
 - (h) "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 Sub-contractors and other suppliers;

- (i) "Cloud Security Principle 9: secure user management" which, amongst other matters, requires the Supplier to make the tools available for the Authority to securely manage the Authority's use of the Service;
- (j) "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;
- (k) "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;
- (l) "Cloud Security Principle 12: secure service administration" which, amongst other matters, requires that any IT system which is used for administration of a cloud service will have highly privileged access to that service;
- (m) "Cloud Security Principle 13: audit information for users" which, amongst other matters, requires the Supplier to be able to provide the Authority with the audit records it needs to monitor access to the Service and the Authority Data held by the relevant Supplier and/or its Sub-contractors;
- (n) "Cloud Security Principle 14: secure use of the service" which, amongst other matters, requires the Supplier to educate the relevant Supplier's Staff on the safe and secure use of the Information Management System.

Appendix B

Security requirements for Sub-contractors

- 1 Application of Appendix
 - 1.1 This Appendix applies to all Sub-contractors that Process Authority Data.
 - 1.2 Each Supplier must:
 - 1.2.1 ensure that those Sub-contractors comply with the provisions of this Appendix;
 - 1.2.2 keep sufficient records to demonstrate that compliance to the Authority; and
 - 1.2.3 ensure that its Detailed Implementation Plan includes Deliverables, Milestones and Milestone Dates that relate to the design, implementation and management of any systems used by Sub-contractors to Process Authority Data.
- 2 Designing and managing secure solutions
 - 2.1 The Sub-contractor 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 Sub-contractor must assess their systems against the NCSC Cloud Security Principles: <https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloud-security/implementing-the-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 Sub-contractor must document that assessment and make that documentation available to the Authority on the Authority's request.
- 3 Data Processing, Storage, Management and Destruction
 - 3.1 The Sub-contractor must not Process any Authority Data outside the UK. The Authority may permit the Sub-contractor to Process Authority Data outside the UK and may impose conditions on that permission, with which the Sub-contractor must comply. Any permission must be in writing to be effective.
 - 3.2 The Sub-contractor must when requested to do so by the Authority:
 - 3.2.1 securely destroy Authority Data only on Sites which are included within the scope of an existing certification of compliance with ISO/IEC 27001;
 - 3.2.2 satisfy the Authority that their data destruction/deletion practices comply with UK GDPR requirements and follows all relevant NCSC guidance; and
 - 3.2.3 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 Sub-contractor 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 Sub-contractor must, if the Authority requires, at any time, ensure that one or more of the Sub-contractor's staff obtains Security Check clearance in order to Process Authority Data

containing Personal Data above certain volumes specified by the Authority, or containing Special Category Personal Data.

- 4.3 Any Sub-contractor 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 Each Supplier must manage, and must ensure that all Sub-contractors manage, all End-User Devices in accordance with the following requirements:

- 5.1.1 the operating system and any applications that Process or have access to Authority Data must be in current support by the vendor, or the relevant community in the case of Open Source operating systems or applications;
- 5.1.2 users must authenticate before gaining access;
- 5.1.3 all Authority Data must be encrypted using an encryption tool agreed to by the Authority;
- 5.1.4 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;
- 5.1.5 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 Authority Data;
- 5.1.6 the Supplier or Sub-contractor, as applicable, can, without physical access to the End-User Device, remove or make inaccessible all Authority Data on the device and prevent any user or group of users from accessing the device; and
- 5.1.7 all End-User Devices are within in the scope of any current Cyber Essentials Plus certificate held by the relevant Supplier, or any ISO/IEC 27001 certification issued by a UKAS-approved certification body, where the scope of that certification includes the Services.

- 5.2 Each Supplier must comply, and ensure that all Sub-contractors 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 Contract.

- 5.3 Where there any conflict between the requirements of this Schedule 5 (Security Management) and the requirements of the NCSC Device Guidance, the requirements of this Schedule will take precedence.

6 Encryption

- 6.1 Each Supplier must ensure, and must ensure that all Sub-contractors ensure, that Authority Data is encrypted:

- 6.1.1 when stored at any time when no operation is being performed on it; and
- 6.1.2 when transmitted.

- 6.2 Where either Supplier, or a Sub-contractor, cannot encrypt Authority Data the relevant Supplier must:

- 6.2.1 immediately inform the Authority of the subset or subsets of Authority Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;

- 6.2.2 provide details of the protective measures the relevant Supplier or Sub-contractor (as applicable) proposes to take to provide equivalent protection to the Authority as encryption; and
 - 6.2.3 provide the Authority with such information relating to the Authority Data concerned, the reasons why that Authority Data cannot be encrypted and the proposed protective measures as the Authority may require.
- 6.3 The Authority, the relevant Supplier and, where the Authority requires, any relevant Sub-contractor shall meet to agree appropriate protective measures for the unencrypted Authority Data.
- 6.4 Where the Authority and Supplier reach agreement, the relevant Supplier must update the Security Management Plan to include:
 - 6.4.1 the subset or subsets of Authority Data not encrypted and the circumstances in which that will occur; and
 - 6.4.2 the protective measure that the relevant Supplier and/or Sub-contractor will put in place in respect of the unencrypted Authority Data.
- 6.5 Where the Authority and Supplier do not reach agreement within forty (40) Working Days of the date on which the relevant Supplier first notified the Authority that it could not encrypt certain Authority Data, either Party may refer the matter to be determined in accordance with the Dispute Resolution Procedure.
- 7 Patching and vulnerability scanning

The Sub-contractor 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 Sub-contractors
 - 8.1 The Sub-contractor must not transmit or disseminate the Authority Data to any other person unless specifically authorised by the Authority. Such authorisation must be in writing to be effective and may be subject to conditions.
 - 8.2 The Sub-contractor must not, when performing any part of the Services, use any software to Process Authority Data where the licence terms of that software purport to grant the licensor rights to Process the Authority Data greater than those rights strictly necessary for the use of the software.

Appendix C

[REDACTED]

REDACTED