CONTRACT FOR PRISONER AND NON-PRISONER FOOD SUPPLY

SCHEDULE 5

SECURITY MANAGEMENT

Part A: Security Assurance

1. Definitions

1.1 In this Schedule:

"Anti-Malicious Software"	means software that scans for and identifies possible Malicious Software in the IT Environment;
"Breach of Security	an event that results, or could result, in: (a) any unauthorised access to or use of the Authority Data, the Services and/or the Information Management System; and/or (b) the loss, corruption and/or unauthorised disclosure of any information or data (including the Confidential Information and the Authority Data), including any copies of such information or data, used by the Authority and/or the Supplier in connection with this Agreement;
"Certification Requirements"	means the information security requirements set out in Paragraph 6;
"CHECK Service Provider"	means a company which has been certified by the National Cyber Security Centre, holds "Green Light" status and is authorised to provide the IT Health Check services required by Paragraph 7.1;
"CREST Service Provider"	means a company with a SOC Accreditation from CREST International;
"Higher Risk Sub-contractor"	means a Sub-contractor that Processes Authority Data, where that data includes either: (a) the Personal Data of 1000 or more individuals in aggregate during the period between the Supply Commencement Date and the date on which this Agreement terminates or expires; or (b) any part of that data includes any of the following: (i) financial information (including any tax and/or welfare information) relating to any person; (ii) any information relating to actual or alleged criminal offences (including criminal records); (iii) any information relating to children and/or vulnerable persons; (iv) any information relating to social care; (v) any information relating to a person's current or past employment; or (vi) Special Category Personal Data; or (c) the Authority in its discretion, designates a Sub-contractor as a Higher Risk Sub-Contractor in any procurement document related to this Agreement; or

(d) the Authority considers in its discretion, that any actual or potential Processing carried out by the Sub-contractor is high risk

"Cyber Essentials"	means the Cyber Essentials certificate issued under the Cyber Essentials Scheme;
"Cyber Essentials Plus"	means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme;
"Cyber Essentials Scheme"	means the Cyber Essentials scheme operated by the National Cyber Security Centre;
"Incident Management Process"	means the process which the Supplier shall implement immediately after it becomes aware of a Breach of Security which is intended to restore normal operations as quickly as possible, minimising any adverse impact on the Authority Data, the Authority, the Services, the delivery of the Products and/or users of the Services of Products and which shall be shall be prepared by the Supplier in accordance with Paragraph 4 using the template set out in Annex 3;
"Information Assurance Assessment"	means the set of policies, procedures, systems and processes which the Supplier shall implement, maintain and update in accordance with Paragraph 4 in order to manage, mitigate and, where possible, avoid information security risks including cyber-attacks, hacks, data leaks, Data Loss Events and/or theft and which shall be prepared by the Supplier using the template set out in Annex 3;
"Information Management System"	means (a) those parts of the Supplier System, and those of the Sites, that the Supplier or its Sub-contractors will use to provide the parts of the Services that require Processing Authority Data; and (b) the associated information assets and systems (including organisational structure, controls, policies, practices, procedures, processes and resources);
"Information Security Approval Statement"	means a notice issued by the Authority which sets out the information risks which the Supplier has identified as being associated with using the Information Management System and confirms that: (a) the Authority is satisfied that the identified risks have been adequately and appropriately addressed; (b) the Authority has accepted the residual risks; and (c) the Supplier may use the Information Management System to Process Authority Data;
"IT Health Check"	has the meaning given in Paragraph 7.1.1;
"Medium Risk Sub-contractor"	means a Sub-contractor that Processes Authority Data, where that data:

	(a) includes the Personal Data of between 100 and 999 individuals (inclusive) in the period between the Supply Commencement Date and the date on which this Agreement terminates or expires; and (b) does not include Special Category Personal Data;
"Process"	means any operation which is performed on data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
"Remediation Action Plan"	has the meaning given in Paragraph 7.3.3(a);
"Required Changes Register"	mean the register within the Security Management Plan which is to be maintained and updated by the Supplier and which shall record each of the changes that the Supplier shall make to the Information Management System and/or the Security Management Plan as a consequence of the occurrence of any of the events set out in Paragraph 5.2 together with the date by which such change shall be implemented and the date on which such change was implemented;
"Risk Register"	is the risk register within the Information Assurance Assessment which is to be prepared and submitted to the Authority for approval in accordance with Paragraph 4;
"Security Management Plan"	means the document prepared by the Supplier using the template in Annex 3, comprising: (a) the Information Assurance Assessment; (b) the Required Changes Register; and (c) the Incident Management Process;
"Special Category Personal Data"	means the categories of Personal Data set out in article 9(1) and article 10 of the UK GDPR;

2. Introduction

2.1 This **Part A** of this Schedule sets out:

2.1.1 the arrangements the Supplier must implement before, and comply with when, providing the Services and delivering the Products and performing its other obligations under this Agreement to ensure the security of the Authority Data and the Information Management System;

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

2.1.3 the security requirements in Annex **1**, with which the Supplier must comply;

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

2.1.5 the Supplier's obligations to:

(a) return or destroy Authority Data on the expiry or earlier termination of this Agreement; 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 9; and

(c) report Breaches of Security to the Authority.

3. Principles of Security

3.1 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:

3.1.1 the Sites;

3.1.2 the IT Environment;

3.1.3 the Information Management System; and

3.1.4 the Services.

3.2 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:

3.2.1 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

3.2.2 the security of the Information Management System.

3.3 The Supplier shall:

3.3.1 comply with the security requirements in Annex 1; and

3.3.2 ensure that each Sub-contractor that Processes Authority Data complies with the Sub-contractor Security Requirements.

3.4 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.

4. Information Security Approval Statement

4.1 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 Annex 2, from the Supply Commencement Date.

4.2 The Supplier may not use the Information Management System to Process Authority Data unless and until:

4.2.1 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 7.1; and

4.2.2 the Authority has issued the Supplier with an Information Security Approval Statement in accordance with the process set out in this Paragraph 4.

4.3 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 Agreement in order to ensure the security of the Authority Data and the Information Management System.

4.4 The Supplier shall prepare and submit to the Authority within 20 Working Days of the date of this Agreement, the Security Management Plan, which comprises:

4.4.1 an Information Assurance Assessment;

4.4.2 the Required Changes Register; and

4.4.3 the Incident Management Process.

4.5 The Authority shall review the Supplier's proposed Security Management Plan as soon as possible and, in any event within 20 Working Days of receipt and shall either issue the Supplier with:

4.5.1 an Information Security Approval Statement, which shall confirm that the Supplier may use the Information Management System to Process Authority Data; or

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

4.6 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 10 Working Days or such other timescale as agreed with the Authority.

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

4.7.1 access to the Supplier Personnel;

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

4.7.3 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 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.

5. Compliance Reviews

5.1 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.

5.2 The Supplier shall notify the Authority within 2 Working Days after becoming aware of:

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

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

5.2.3 a vulnerability to the components or architecture of the Service which is classified 'Medium', 'High', 'Critical' or 'Important' in accordance with the classification methodology set out in Paragraph 9.2 of Annex 1 to this Schedule;

5.2.4 a change in the threat profile;

5.2.5 a significant change to any risk component;

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

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

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

5.3 Within 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 the Authority for review and approval.

5.4 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.

6. Certification Requirements

6.1 The Supplier shall be certified as compliant with:

6.1.1 NOT USED;

6.1.2 Cyber Essentials PLUS,

and shall provide the Authority with a copy of such certificate of compliance before the Supplier shall be permitted to receive, store or Process Authority Data.

6.2 The Supplier shall ensure that each Higher Risk Sub-contractor is certified as compliant with:

6.2.1 NOT USED;

6.2.2 Cyber Essentials PLUS,

and shall provide the Authority with a copy of such certificate of compliance before the Higher-Risk Sub-contractor shall be permitted to receive, store or Process Authority Data.

6.3 The Supplier shall ensure that each Medium Risk Sub-contractor is certified compliant with Cyber Essentials.

6.4 The Supplier shall ensure that the Supplier and each Sub-contractor who is responsible for the secure destruction of Authority Data:

6.4.1 NOT USED;

6.4.2 should satisfy the Authority that their data destruction/deletion practices comply with UK GDPR requirements and follows all relevant NCSC guidance; and

6.4.3 must maintain an asset register of all Authority supplied information, data and equipment to ensure Authority assets are returned and/or deleted.

6.5 The Supplier shall provide the Authority with evidence of its and its Sub-contractor's compliance with the requirements set out in this Paragraph 6 before the Supplier or the relevant Sub-contractor (as applicable) may carry out the secure destruction of any Authority Data.

6.6 The Supplier shall notify the Authority as soon as reasonably practicable and, in any event within 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:

6.6.1 immediately ceases using the Authority Data; and

6.6.2 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.

6.7 The Authority may agree to exempt, in whole or part, the Supplier or any Sub-contractor from the requirements of this Paragraph 6. Any exemption must be in writing to be effective. The Supplier must include the exemption in the Security Management Plan.

7. Security Testing

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

7.1.1 testing of the Information Management System by a CHECK Service Provider or a CREST Service Provider ("**IT Health Check**"); and

7.1.2 such other security tests as may be required by the Authority,

7.2 The Supplier shall:

7.2.1 complete all of the above security tests before:

(a) the Supplier submits the Security Management Plan to the Authority for review in accordance with Paragraph 4; and

(b) before the Supplier is given permission by the Authority to Process or manage any Authority Data; and

7.2.2 repeat the IT Health Check not less than once every 12 months during the Term and submit the results of each such test to the Authority for review in accordance with this Paragraph.

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

7.3.1 agree with the Authority the aim and scope of the IT Health Check;

7.3.2 promptly, and no later than ten (10) Working Days, following the receipt of each IT Health Check report, provide the Authority with a copy of the full report;

7.3.3 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:

(b) how the vulnerability will be remedied;

(c) unless otherwise agreed in writing between the Parties, the date by which the vulnerability will be remedied, which must be:

(d) within three months of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of "medium";

(e) within one month of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of "high"; and

(f) within 7 Working Days of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of "critical";

(g) 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;

(h) comply with the Remediation Action Plan; and

(i) 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.

7.4 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 Products and the date, timing, content and conduct of such tests shall be agreed in advance with the Authority.

7.5 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 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:

7.5.1 propose interim mitigation measures to vulnerabilities in the Information Management System known to be exploitable where a security patch is not immediately available; and

7.5.2 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 or delivery of the Products (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.

7.6 The Supplier shall conduct such further tests of the Supplier System as may be required by the Authority from time to time to demonstrate compliance with its obligations set out this Schedule and the Agreement.

7.7 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 7.3.

8. Security Monitoring and Reporting

8.1 The Supplier shall:

8.1.1 monitor the delivery of assurance activities;

8.1.2 maintain and update the Security Management Plan in accordance with Paragraph 5;

8.1.3 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;

8.1.4 monitor security risk impacting upon the operation of the Service;

8.1.5 report Breaches of Security in accordance with the approved Incident Management Process;

8.1.6 agree with the Authority the frequency and nature of the security reports to be prepared and submitted by the Supplier to the Authority within 20 Working Days of Effective Date.

9. Malicious Software

9.1 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.

9.2 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 and delivery of Products to their desired operating efficiency.

9.3 Any cost arising out of the actions of the parties taken in compliance with the provisions of Paragraph 9.2 shall be borne by the parties as follows:

9.3.1 by the Supplier where the Malicious Software originates from:

(a) the Supplier Software;

(b) any 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

9.3.2 by the Authority, in any other circumstance.

10. Breach of Security

10.1 If either party becomes aware of a Breach of Security it shall notify the other in accordance with the Incident Management Process.

10.2 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:

10.2.1 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;

10.2.2 as soon as reasonably practicable and, in any event, within 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.

10.3 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 Agreement, then such remedial action shall be completed at no additional cost to the Authority.

Annex 1: Security Requirements

1. Security Classification of Information

1.1 If the provision of the Services or delivery of the Products requires the Supplier to Process Authority Data which is classified as:

1.1.1 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

1.1.2 SECRET or TOP SECRET, the Supplier shall only do so where it has notified the Authority prior to receipt of such Authority Data and the Supplier shall 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 used by the Supplier on which Authority Data is Processed in accordance 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 the scope of any current Cyber Essentials Plus certificate held by the Supplier, where the scope of that certification includes the Services or delivery of the Products.

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 Agreement.

2.3 Where there is 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 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 or delivery of the Products. 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; verification of the individual's employment history; and subject to Paragraph 4.2 below, verification of the individual's criminal record.

4.2 The Supplier shall not be required to carry out criminal record vetting in relation to the following categories of Supplier Personnel:

4.2.1 Supplier Personnel who undertake work solely at the Supplier's depots; and

4.2.2 Supplier Personnel who do not have access to Authority Data classified as OFFICIAL SENSITIVE or any higher security rating.

4.3 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 or delivery of the Products 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.

4.4 The Supplier shall not permit Supplier Personnel who fail the security checks required by Paragraphs 4.1 and 4.3 to be involved in the management and/or provision of the Services or delivery of the Products 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 or delivery of the Products.

4.5 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.

4.6 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 1 Working Day.

4.7 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.

4.8 The Supplier shall ensure that the training provided to Supplier Staff under Paragraph 4.7 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 format provided it is secure and readable;

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 and certify to the Authority that it has done so unless and to the extent required by Law to retain it other than in relation to Authority Data which is owned or licenced by the Supplier or in respect of which the Parties are either Independent Controllers or Joint Controllers;

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 Agreement and, in the absence of any such requirements, as agreed by the Authority other than in relation to Authority Data which is owned or licenced by the Supplier or in respect of which the Parties are either Independent

Controllers or Joint Controllers; 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

8.1 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 as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the agreed method in the Security Management Plan and using the appropriate vulnerability scoring systems including:

9.2.1 the 'National Vulnerability Database' 'Vulnerability Severity Ratings': 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS scores as set out by NIST at http://nvd.nist.gov/cvss.cfm); and

9.2.2 Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.

9.3 Subject to Paragraph 9.4, the Supplier shall procure the application of security patches to vulnerabilities in the Information Management System within:

9.3.1 seven (7) days after the public release of patches for those vulnerabilities categorised as 'Critical';

9.3.2 thirty (30) days after the public release of patches for those vulnerabilities categorised as 'Important'; and

9.3.3 sixty (60) days after the public release of patches for those vulnerabilities categorised as 'Other'.

9.4 The timescales for applying patches to vulnerabilities in the Information Management System set out in Paragraph 9.3 shall be extended where:

9.4.1 the Supplier can demonstrate that a vulnerability in the Information Management System is not exploitable within the context of the Services of Products (e.g. because it resides in a Software component which is not involved in running in the Services or

delivery of the Products) 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 or Products;

9.4.2 the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services or Products 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.

11. Changes to Security Requirements

11.1 The Authority may, from time to time, update the security requirements set out in this Annex 1 by giving the Supplier reasonable written notice. The Supplier shall, as soon as reasonably practicable, incorporate and comply with such revised security requirements.

Annex 2: Security Requirements for Sub-Contractors

1. Application of Annex 2

1.1 This Annex 2 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 Annex 2;

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 NOT USED;

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 or delivery of the Products. 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 or delivering the Products, 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 on which Authority Data is Processed in accordance 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 the scope of any current Cyber Essentials Plus certificate held by the Supplier, where the scope of that certification includes the Services or delivery of the Products.

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 Agreement.

5.3 Where there is 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 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

7.1 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 or delivering the Products, use any software to Process the Authority Data where the licence terms of that software purport to grant the licensor rights to Progress the Authority Data greater than those rights strictly necessary for the use of the software.

Annex 3: Security Management Plan Template

Security Management Plan Template

[Project/Service and Supplier Name]

1. Executive Summary

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

2. System Description

2.1 Background

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

2.2 Organisational Ownership/Structure

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

2.3 Information assets and flows

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

2.4 System Architecture

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

2.5 Users

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

2.6 Locations

[Where the data assets are stored and managed from. If any locations hold independent security certifications 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 B should contain the output of the formal information risk assessment in a prioritised list using business language. Experts on the system and business process should have been involved in the risk assessment to ensure the formal risk methodology used has not missed out any risks. The example table below should be used as the format to identify the risks and document the controls used to mitigate those risks.]

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

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

3.5 Controls

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

ID	Control title	Control description	Further information and assurance status
C1	Internet-facing firewalls	Internet-facing firewalls are in place between the internet and the system', which restrict access from the internet to the required ports only.	Assured via ITHC firewall rule check
C2	Internet-facing IP whitelist	An IP whitelist is in place for all access from the internet.	Assured via ITHC
C15	Staff awareness training	All staff must undertake annual security awareness training and this process is audited and monitored by line managers.	N/A

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 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)

5.1 [If needed any SyOps requirements should be included and referenced here.]

6. Major Hardware and Software and end of support dates

6.1 [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

7.1 [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

8.1 [Any security requirements for connecting organisations or departments should be included or referenced here.]

9. Required Changes Register

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

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

10. Sub-contractors

10.1 [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. Cyber Essential Plus certificates

11.1 [Any certifications relied upon should have their certificates included]

12. Annex B. Cloud Security Principles assessment

12.1 [A spreadsheet may be attached]

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

13.1 [A spreadsheet may be attached]

14. Annex D. Latest ITHC report and Remediation Action Plan