Call Off Schedule 9 (Security Requirements)

1. **Definitions**

In this Schedule, the following definitions shall apply and be supplemental to those in Joint Schedule 1 (Definitions):

"Accreditation"	the assessment of the Core Information Management System in accordance with Part C of this Schedule by the Buyer or an independent information risk manager/professional appointed by the Buyer, which results in an Accreditation Decision;
"Accreditation Decision"	is the decision of the Buyer, taken in accordance with the process set out in Paragraph 4 of Part C of this Schedule, to issue the Supplier with a Risk Management Approval Statement or a Risk Management Rejection Notice in respect of the Core Information Management System;
"Accreditation Plan"	the Supplier's plan to attain an Accreditation Approval Statement from the Buyer, which is prepared by the Supplier and Approved by the Buyer in accordance with Part C of this Schedule;
“Anti-Malicious Software”	Software that scans for and identifies possible Malicious Software in the ICT Environment;
"Breach of Security"	the occurrence of: (a) any unauthorised access to or use of the Services, the Sites, the Supplier System, and/or any information or data (including the Confidential Information and the Government Data) used by the Buyer, the Supplier or any Subcontractor in connection with this Call-Off Contract; (b) the loss (physical or otherwise) and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including copies of such information or data, used by the Buyer, the Supplier and/or any Subcontractor in connection with this Call-Off Contract; and/or (c) any part of the Supplier System ceasing to be compliant with the Certification Requirements, in each case as more particularly set out in the Security Requirements in Framework Schedule

Call Off Schedule 9 (Security Requirements)
Call Off Ref: [Redacted]

	1 (Specification) and the Order Form and the Security Requirements;
"Certification Requirements"	the requirements set out in Part E of this Schedule;
“CHECK Service Provider”	a company which has been certified by the National Cyber Security Centre, holds "Green Light" status and is authorised to provide the ITHC Services required by the Paragraph 4.2 of Part C of this Schedule;
“CIMS Subcontractor”	a Subcontractor that provides or operates the whole, or a substantial part, of the Core Information Management System;
"Core Information Management System"	those information assets, ICT systems and/or Sites which will be used by the Supplier and/or its Subcontractors to Process Government Data, together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources) which the Buyer has determined in accordance with the Security Requirements;
General Security Requirements	the Security Requirements that shall apply to any Supplier and / or Subcontractor that processes Personal Data;
“Higher Risk Subcontractor”	a Subcontractor that Processes Government Data, where that data includes either: (a) the Personal Data of 1000 or more individuals in aggregate during the period between the Call-Off Start Date and the End Date; or (b) Special Category Personal Data, other than information about the access or dietary requirements of the individuals concerned;
"IT Health Check" (ITHC)	has the meaning given Paragraph 4.2 of Part C of this Schedule;
Incident Management Process	is the process which the Supplier shall implement immediately after it becomes aware of a Breach of Security which is intended to restore normal operations as quickly as possible, minimising any adverse impact on the Government Data, the Buyer, the Services and/or users of the Services and which shall be prepared by the Supplier in accordance with Paragraph 13.2 of Part A of this

	Schedule and as set out by the Supplier and Approved by the Buyer within the template set out in Section 23 of Appendix 1 of this Schedule;
"Information Assurance Assessment"	is the set of policies, procedures, systems and processes which the Supplier shall implement, maintain and update in accordance with Part B of this Schedule in order to manage, mitigate and, where possible, avoid information security risks including cyber-attacks, hacks, data leaks, Personal Data Breaches and/or theft and which shall be prepared by the Supplier using the template set out in Appendix 1 of this Schedule;
"Information Management System"	the Core Information Management System and the Wider Information Management System;
"Information Security Approval Statement"	a notice issued by the Buyer which sets out the information risks which the Supplier has identified as being associated with using the Information Management System and confirms that the Buyer: (i) is satisfied that the identified risks have been adequately and appropriately addressed; (ii) the Buyer has accepted the residual risks; and (iii) the Supplier may use the Information Management System to Process Government Data;
"Malicious Software"	any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence;
"Medium Risk Subcontractor"	a Subcontractor that Processes Government Data, where that data (a) includes the Personal Data of between 100 and 999 individuals (inclusive) in the period between the Call-Off Start Date and the End Date; and (b) does not include Special Category Personal Data, other than information about the access or dietary requirements of the individuals concerned;

"Required Changes Register"	is a register which forms part of the Risk Management Documentation which records each of the changes that the Supplier has agreed with the Buyer to be made to the Core Information System and/or the Security Management Plan as a consequence of the occurrence of any of the events set out in the following Paragraphs within: ● 1.3 of Part B; ● 4 of Part C; ● 3 of Part D; together with the date on which each change shall be implemented and the date on which each change was implemented;
"Risk Management Approval Statement"	a notice issued by the Buyer which sets out the information risks associated with using the Core Information Management System and confirms that the Buyer is satisfied that the identified risks have been adequately and appropriately addressed and that the residual risks are understood and accepted by the Buyer;
"Risk Management Documentation"	is the information and supporting documentation that the Supplier develops and provides to the Buyer when completing section 11 of the Security Management Plan;
"Risk Management Reject Notice"	has the meaning given in Paragraph 4.8.2;
“Security Management Plan”	comprises all information required from the Supplier in order to demonstrate compliance with the Security Requirements that must be presented in the templates set out in Appendix 1;
Security Requirements	the security requirements that the Supplier and each Subcontractor must comply with during the Contract Period as set out in the this Schedule;
"Security Test"	has the meaning given Paragraphs 4 in Part C and Part D of this Schedule;
Security Working Group	the meeting led by the Buyer (or their agent) with the Supplier to discuss the Security Management Plan and any risks, issues and controls the Supplier has put into place to ensure they are delivering the Security Requirements. The timing, required attendees and periodicity of the meetings will be defined by the Buyer during implementation, but should be no less than

	quarterly and should include the Supplier's Staff with the relevant expertise;
"Special Category of Personal Data"	the categories of Personal Data set out in Article 9(1) of GDPR;
"Statement of Information Risk Appetite"	the document that sets-out the type and level of risk that the Buyer is prepared to accept;
"Subcontractor Security Requirements"	any Security Requirements that must be delivered by Subcontractors;
"Vulnerability Correction Plan"	has the meaning given in Paragraph Part C Paragraph 4.3.3.1 of this Schedule;
"Wider Information Management System"	those information assets, ICT systems and/or Sites which will be used by the Supplier and/or its Subcontractors to Process Government Data which have not been determined by the Buyer to form part of the Core Information Management System together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources).

2. Part A Introduction

2.1. This Schedule sets out:

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

2.1.2. the Certification Requirements applicable to the Supplier and each of those Subcontractors which Processes Government Data;

2.1.3. the Security Requirements with which the Supplier must comply, which are dependent upon the applicable Lot(s) awarded to the Supplier under the Framework Contract;

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

2.1.5. the Supplier's obligations to:

2.1.5.1. return or destroy Government Data on the expiry or earlier termination of this Call-Off Contract; and

2.1.5.2. prevent the introduction of Malicious Software into the Supplier System and to scan for, contain the spread of, and minimise the impact of Malicious Software which is introduced into the Supplier System in Paragraph 8; and

2.1.5.3. report Breaches of Security to the Buyer.

2.1.6. the applicable Tier of Security Requirements required to be complied with by the Supplier are summarised in Table 1 below:

Table 1:

Tier	Lot	Summary Security Requirements	Certification Requirements
1.	2, 3, 8, 9, 10, 11, 12, 13, 14	General Security Requirements (Part B)	ISO 27001:2017 and CE+

3. **Principles of Security**

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

3.1.1. the Sites;

3.1.2. the Supplier System;

3.1.3. the Information Management System, Core information Management System and Wider Information Management System, as applicable; and

3.1.4. the Services.

3.2. Notwithstanding the involvement of the Buyer in assessing the arrangements which the Supplier shall implement in order to ensure the security of the Government 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 Government Data whilst that Government Data is under the control of the Supplier or any of its Subcontractors; 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 this Schedule; and

3.3.2. ensure that each Subcontractor that Processes Government Data complies with the Subcontractor Security Requirements in this Schedule.

3.4. The Supplier shall provide the Buyer with access to Supplier Staff responsible for information assurance to facilitate the Buyer's assessment of the Supplier's compliance with its obligations set out in this Schedule at reasonable times on reasonable notice.

3.5. The Buyer may at its sole discretion appoint an agent to act on it's behalf with regards to its engagement with the Supplier regarding the Security Requirements.

Part B General Security Requirements

1. The Security Management Plan

1.1 The Security Management Plan includes details of each of the tasks which must be completed by the Supplier, Milestones which must be Achieved and the Buyer responsibilities which must be completed in order for the Supplier to receive a Risk Management Approval Statement.

1.2 The Supplier shall complete the Security Management Plan Template (Appendix 1) detailing how they will deliver the Security Requirements and the necessary information required for the applicable Tier(s) for the Lot(s) awarded to the Supplier. Any element that does not apply or only partially applies should be explained within the Template. If a Supplier is delivering Services in respect of more than 1 Lot, it must complete a separate Security Risk Management Template for each Lot.

1.3 Where there has been a Variation or Change to the Services which affects any aspect of the Security Requirements, CCS and the relevant Buyers must be notified immediately in writing of this fact and the extent of its effect or believed effect on the Security Requirements and / or the Tier of the Security Requirements that the Supplier should apply to the Service (actual or potential).

1.4 The Supplier shall complete the Security Management Plan to demonstrate and document how they comply with the Security Requirements. A draft Security Management Plan shall be made available to the Buyer prior to the Call-Off Contract Effective Date unless already Approved by the Buyer.

1.5 The Security Management Plan should be provided to the Buyer in accordance with the Buyer's requirements and as set out within the Implementation Plan, but in any case, unless already Approved by the Buyer, this should be prior to the Service Effective Date.

2. Security Classification of Information

2.1 If the provision of the Services requires the Supplier to Process Government Data which is classified as: OFFICIAL-SENSITIVE, the Supplier shall implement such additional measures as agreed with the Buyer from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards.

3. End User Devices

3.1 The Supplier shall ensure that any Government Data which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the Buyer, except where the Buyer has already Approved a suitable alternative arrangement.

3.2 The Supplier shall ensure that any device which is used to Process Government Data meets all of the Security Requirements set out in the NCSC End User Devices Platform

Security Guidance, a copy of which can be found at: https://www.ncsc.gov.uk/guidance/end-user-device-security

3.3 The Supplier must ensure that their EUD's require all Supplier Staff to authenticate themselves before gaining access to the device. All the Supplier's EUD's must encrypt all data at rest using a reputable full disk encryption solution that has been formally assured through a recognised certification process agreed with the Buyer, except where the Buyer has already Approved a suitable alternative arrangement. The Supplier's EUD's must be configured to automatically lock the screen after a period of inactivity and this must be agreed with the Buyer in writing.

4. **Location of Government Data**

4.1 The Supplier shall not and shall procure that none of its Subcontractors Process Government Data outside the UK without the Approval of the Buyer, which may be subject to conditions and that it shall comply with Joint Schedule 11 (Processing Data).

Call Off Schedule 9 (Security Requirements)
Call Off Ref: [Redacted]

5. **Vulnerabilities and Corrective Action**

5.1 The Buyer and the Supplier acknowledge that from time to time vulnerabilities in the Information Management System will be discovered which unless mitigated will present an unacceptable risk to the Government Data.

5.2 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.

5.3 The Supplier shall utilise scoring according to the agreed method in the Security Management Plan and using the appropriate vulnerability scoring systems including:

5.3.1 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

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

5.4 Subject to Paragraph 5.5, the Supplier shall procure the application of security patches to vulnerabilities in the Information Management System within:

5.4.1 7 days after the public release of patches for those vulnerabilities categorised as 'Critical';

5.4.2 30 days after the public release of patches for those vulnerabilities categorised as 'Important'; and

5.4.3 60 days after the public release of patches for those vulnerabilities categorised as 'Other'.

5.5 The timescales for applying patches to vulnerabilities in the Information Management System set out in Paragraph 5.4 shall be extended where:

5.5.1 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 5.4 if the vulnerability becomes exploitable within the context of the Services;

5.5.2 the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of 5 days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Buyer;

5.5.3 the Buyer Approves to a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the Security Management Plan; or

5.5.4 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 Contract Period, unless otherwise Approved

by the Buyer. All COTS Software should be no more than N-1 versions behind the latest software release.

6. **Networking**

6.1 The Supplier shall ensure that any Government Data which it causes to be transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted using TLS version 1.2 as a minimum.

7. **Personnel Security**

7.1 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.

7.2 The Buyer and the Supplier shall review the roles and responsibilities of the Supplier Staff who will be involved in the management and/or provision of the Services in order to enable the Buyer to determine which roles require additional vetting and a specific national security vetting clearance (e.g. a Counter Terrorist Check; a Security Check). Roles which are likely to require additional vetting and a specific national security vetting clearance include system administrators whose role would provide those individuals with privileged access to IT systems which Process Government Data or data which is classified as OFFICIAL-SENSITIVE.

7.3 The Supplier shall not permit Supplier Staff who fail the security checks required by Paragraphs 7.1 and 7.2 to be involved in the management and/or provision of the Services except where the Buyer Approves the involvement of the named individual in the management and/or provision of the Services.

7.4 The Supplier shall ensure that Supplier Staff are only granted such access to Government Data as is necessary to enable the Supplier Staff to perform their role and to fulfil their responsibilities.

7.5 The Supplier shall ensure that Supplier Staff who no longer require access to the Government Data (e.g. they cease to be employed by the Supplier or any of its Subcontractors), have their rights to access the Government Data revoked within 1 Working Day

8. **Identity, Authentication and Access Control**

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

8.1.1 all users and administrators of the Supplier System are uniquely identified and authenticated when accessing or administering the Services; and

8.1.2 all persons who access the Sites are identified and authenticated before they are allowed access to the Sites.

8.2 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 to perform the Services under the Contract.

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

9. **Audit and Protective Monitoring**

9.1 The Supplier shall collect audit records which relate to security events in the 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 Government Data.

9.2 The Supplier and the Buyer shall work together to establish any additional audit and monitoring requirements for the Core Information Management System.

9.3 The retention periods for audit records and event logs must be agreed with the Buyer and documented in the Security Management Plan.

10. **Secure Architecture**

10.1 The Supplier shall design the Core 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

11. **Malicious Software**

11.1 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 Government 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 Government 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 11.1 shall be borne by the Parties as follows:

11.3.1 by the Supplier where the Malicious Software originates from the Supplier Software, the Third Party Software supplied by the Supplier or the Government Data (whilst the Government Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Buyer when the Data was provided to the Supplier, unless the Buyer had instructed the Supplier to quarantine and check the data for Malicious Software and the Supplier had failed to do so, and

11.3.2 by the Buyer, in any other circumstance.

12. **Data Destruction or Deletion**

12.1 The Supplier shall:

12.1.1 prior to securely sanitising any Government Data or when requested the Supplier shall provide the Buyer with two copies of all Buyer Data in an agreed open format;

12.1.2 have documented processes to ensure the availability of Government Data in the event of the Supplier ceasing to trade;

12.1.3 securely erase in a manner agreed with the Buyer any or all Government Data held by the Supplier when requested to do so by the Buyer;

12.1.4 securely destroy in a manner agreed with the Buyer all media that has held Government Data at the end of life of that media in accordance with any specific

requirements in this Call-Off Contract and, in the absence of any such requirements, as agreed by the Buyer in writing; and

12.1.5 implement processes which address the CPNI and NCSC guidance on secure sanitisation.

13. **Breach of Security**

13.1 If either Party becomes aware or reasonably suspects of a Breach of Security it shall notify the other in accordance with the Incident Management Process.

13.2 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:

13.2.1 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;

13.2.2 as soon as reasonably practicable and, in any event, within twelve (12) hours following the Breach of Security or attempted Breach of Security, the Supplier must provide to the Buyer full details of the Breach of Security or attempted Breach of Security, including a root cause analysis as required by the Buyer.

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

14. **Security Monitoring and Reporting**

14.1 The Supplier shall:

14.1.1 monitor the delivery of assurance activities;

14.1.2 maintain and update the Security Management Plan in accordance with Paragraph 1;

14.1.3 agree a document which presents the residual security risks to inform the Buyer's decision on whether or not to give Approval to the Supplier to Process, store and transit the Government Data;

14.1.4 monitor security risk impacting upon the operation of the Service, including by completing and providing to the Buyer, an information security questionnaire in the format stipulated by the Buyer (and procuring that any Subcontractor completes

such information security questionnaire if requested by the Buyer) as requested by the Buyer, within one calendar month from the date of such request;

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

14.1.6 agree with the Buyer the frequency and nature of the security reports to be prepared and submitted by the Supplier to the Buyer within 30 days of the Start Date of this Call-Off Contract.

Part C Accreditation requirements

1. **This Part sets out:**

1.1 The Accreditation arrangements that the Supplier must implement and comply with when providing the Services and performing its other obligations under this Call-Off Contract. These are required to ensure the security of the Government Data, the ICT Environment, the Services and the Information Management System, which are in addition to the requirements set-out in Parts A, B and E and Appendix 1 and 2 of this Schedule.

1.2 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.

1.3 The Supplier shall provide access to the Supplier Staff responsible for information assurance and the Buyer shall provide access to its Personnel responsible for information assurance, at reasonable times upon reasonable written notice.

2. **Information Management System**

2.1. The Information Management System comprises the Core Information Management System and the Wider Information Management System.

2.2. The Buyer shall be responsible for determining the boundary between the Core Information Management System and the Wider Information Management System. In order to enable the Buyer to make such determination, the Supplier shall provide the Buyer with such documentation and information that the Buyer may reasonably require regarding any information assets, ICT systems and/or Sites which will be used by the Supplier or any Subcontractor to Process Government Data together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources). The Buyer shall notify the Supplier, as soon as reasonably practical following the receipt of such documentation and information, of its decision regarding the component parts of the Core Information Management System and its boundary with the Wider Information Management System.

2.3. The Supplier shall reproduce the Buyer's decision as a diagram documenting the Core Information Management System, the Wider Information Management system and the boundary between the two. This diagram shall form part of the Security Management Plan.

2.4. 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 Clause 24 of the Core Terms (Changing the contract).

3. **Statement of Information Risk Appetite and Security Requirements**

3.1. The Supplier acknowledges that the Buyer has provided and the Supplier has received a statement of information risk appetite for the Supplier System and the Services ("**Statement of Information Risk Appetite**").

3.2. The Buyer's Security Requirements in respect of the Core Information Management System shall be set out in Appendix 1 (below).

4. **Accreditation of the Core Information Management System**

4.1. The Core Information Management System shall be subject to Accreditation in accordance with this Paragraph 4.

4.2. The Supplier acknowledges that the purpose of Accreditation is to ensure that:

4.2.1. the Security Management Plan accurately represents the Core Information Management System;

4.2.2. the Accreditation Plan, if followed, provides the Buyer with sufficient confidence that the CIMS will meet the requirements of the Security Requirements and the Statement of Risk Appetite; and

4.2.3. the residual risks of the Core Information Management System are no greater than those provided for in the Statement of Risk Appetite and Security Requirements.

4.3. The Accreditation shall be performed by the Buyer or by representatives appointed by the Buyer.

4.4. In addition to any obligations imposed by Call-Off Schedule 13 (Implementation Plan and Testing), the Supplier must ensure that its Implementation Plan sets out in sufficient detail how it will ensure compliance with the requirements of this Call-Off Schedule 9 (Security Requirements), including any requirements imposed on Subcontractors, from the Call-Off Contract Start Date.

4.5. By the date specified in the Implementation Plan, the Supplier shall prepare and submit to the Buyer the risk management documentation for the Core Information Management System, which shall be subject to approval by the Buyer in accordance with, Part B Paragraph 5 (the "**Security Management Plan**").

4.6. The Supplier must provide, by the date by which the Supplier is required to have received a Risk Management Approval Statement from the Buyer together with:

4.6.1. details of each of the tasks which must be completed by the Supplier, Milestones which must be Achieved and the Buyer responsibilities which must be completed in

order for the Supplier to receive a Risk Management Approval Statement pursuant to Paragraph 4.8.1.

4.6.2. a formal risk assessment of the Core Information Management System and a risk treatment plan for the Core Information Management System;

4.6.3. a completed ISO 27001:2013 Statement of Applicability for the Core Information Management System; the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Services, processes associated with the delivery of the Services, the Buyer Premises, the Sites, the Supplier System, the Buyer System (to extent that it is under the control of or accessed the Supplier) and any IT, Information and data (including the Confidential Information of the Buyer and the Government Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Services; and

4.6.4. unless such requirement is waived by the Buyer, 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 Buyer Premises, the Sites, the Supplier System, the Buyer 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 Buyer and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Call-Off Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Services including:

4.6.4.1. the Required Changes Register;

4.6.4.2. evidence that the Supplier and each applicable Subcontractor is compliant with the Certification Requirements;

4.6.4.3. a Personal Data Processing Statement; and

4.6.4.4. the diagram documenting the Core Information Management System, the Wider Information Management System and the boundary between the two created under Paragraph 3.2.

4.7. To facilitate Accreditation of the Core Information Management System, the Supplier shall provide the Buyer and its authorised representatives with:

4.7.1. 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

4.7.2. such other information and/or documentation that the Buyer or its authorised representatives may reasonably require, to enable the Buyer to establish that the Core Information Management System is compliant with the Security Management Plan.

4.8. The Buyer shall, by the relevant date set out in the Accreditation Plan, review the Security Management Plan and issue to the Supplier either:

4.8.1. a Risk Management Approval Statement which will then form part of the Security Management Plan, confirming that the Buyer 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 Buyer; or

4.8.2. a rejection notice stating that the Buyer 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"**).

4.9. If the Buyer issues a Risk Management Rejection Notice, the Supplier shall, within 20 Working Days of the date of the Risk Management Rejection Notice:

4.9.1. address all of the issues raised by the Buyer in such notice;

4.9.2. update the Security Management Plan, as appropriate, and

4.9.3. notify the Buyer that the Core Information Management System is ready for an Accreditation Decision.

4.10. If the Buyer issues a two or more Risk Management Rejection Notices, the failure to receive a Risk Management Approval Statement shall constitute a material Default and the Buyer may by terminate this Call-Off Contract with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 10.4 of the Core Terms.

4.11. Subject to Paragraph 4.10, the process set out in Paragraphs 4.9 shall be repeated until such time as the Buyer issues a Risk Management Approval Statement to the Supplier or terminates this Call-Off Contract.

4.12. The Supplier shall not use the Core Information Management System to Process Government Data prior to receiving a Risk Management Approval Statement.

4.13. The 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 4 and the Buyer shall review the

Accreditation Decision annually and following the occurrence of any of the events set out in Paragraph 4.9.

4.14. The Supplier shall notify the Buyer within 2 Working Days after becoming aware of:

4.14.1. a significant change to the components or architecture of the Core Information Management System;

4.14.2. a new risk or vulnerability is identified to the components or architecture of the Core Information Management System;

4.14.3. a change in the threat profile;

4.14.4. a Subcontractor failure to comply with the Core Information Management System code of connection;

4.14.5. a significant change to any risk component; and/or

4.14.6. a significant change in the quantity of Personal Data held within the Core Information Management System.

4.15. Where the Supplier has previously Processed Personal Data that does not include Special Category Personal Data, it starts to Process Special Category Personal Data, other than data relating to accessibility or dietary requirements relating to an individual:

4.15.1. a proposal to change any of the Sites from which any part of the Services are provided; and

4.15.2. an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns; and

4.15.3. update the Required Changes Register and provide the updated Required Changes Register to the Buyer for review and Approval within 10 Working Days after the initial notification or such other timescale as may be agreed with the Buyer.

4.16. If the Supplier fails to implement a change which is set out in the Required Changes Register by the date agreed with the Buyer, such failure shall constitute a material Default and the Supplier shall:

4.16.1. immediately cease using the Core Information Management System to Process Government Data until the Default is remedied, unless directed otherwise .by the Buyer in writing and then it may only continue to Process Government Data in accordance with the Buyer's written directions; and

4.16.2. where such Default is capable of remedy, the Supplier shall remedy such Default within the timescales set by the Buyer and, should the Supplier fail to remedy the Default within such timescales, the Buyer may terminate this Call-Off Contract with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 10.4 of the Core Terms

4.17. The 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 Buyer.

4.18. The 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 Buyer as part of the Accreditation process.

5. **Security Testing**

5.1. The Supplier shall, at its own cost and expense:

5.1.1. procure testing of the Core Information Management System by a CHECK Service Provider (an "**IT Health Check**"):

5.1.1.1. prior to it submitting the Security Management Plan to the Buyer for an Accreditation Decision;

5.1.1.2. if directed to do so by the Buyer; and

5.1.1.3. once every 12 Months during the Call-Off Contract Period:

5.1.1.4. conduct vulnerability scanning and assessments of the Core Information Management System Monthly;

5.1.1.5. conduct an assessment as soon as reasonably practicable following receipt by the Supplier or any of its Subcontractors of a critical 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

5.1.1.5.1. conduct such other tests as are required by:

5.1.1.5.2. any Vulnerability Correction Plans;

5.1.1.5.3. the ISO27001 certification requirements;

5.1.1.5.4. the Security Management Plan; and

5.1.1.5.5. The Buyer following a Breach of Security or a significant change to the components or architecture of the Core Information Management System,

(each a "**Security Test**").

5.2. The Supplier shall provide the Buyer with the results of such Security Tests (in a form approved by the Buyer in advance) as soon as practicable, and in any case within 10 Working Days, after completion of each Security Test.

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

5.3.1. agree with the Buyer the aim and scope of the IT Health Check;

5.3.2. promptly, and in any case no later than 10 Working Days, following receipt of each IT Health Check report, provide the Buyer with a copy of the IT Health Check report

5.3.3. in the event that the IT Health Check report identifies any vulnerabilities, the Supplier shall:

5.3.4. prepare a remedial plan for approval by the Buyer (each a "**Vulnerability Correction Plan**") which sets out in respect of each vulnerability identified in the IT Health Check report:

5.3.4.1. how the vulnerability will be remedied;

5.3.4.2. the date by which the vulnerability will be remedied;

5.3.4.3. the tests which the Supplier shall perform or procure to be performed (which may, at the discretion of the Buyer, include a further IT Health Check) to confirm that the vulnerability has been remedied;

5.3.4.4. comply with the Vulnerability Correction Plan; and

5.3.4.5. conduct such further Security Tests on the Core Information Management System as are required by the Vulnerability Correction Plan to confirm that the Vulnerability Correction Plan has been complied with.

5.4. 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 Buyer.

5.5. The Buyer shall be entitled to send a representative to witness the conduct of the Security Tests. Without prejudice to the Supplier's obligations under Paragraph 5.3, the Supplier shall provide the Buyer with the results of such Security Tests (in a form approved by the Buyer in advance) as soon as practicable, and in any case no later than 10 Working Days, after completion of each Security Test.

5.6. The Buyer 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 ("**Buyer Security Tests**"). The Buyer shall take reasonable steps to notify the Supplier prior to carrying out such Buyer Security Test to the extent that it is reasonably practicable for it to do so taking into account the nature and purpose of the Buyer Security Test.

5.7. The Buyer shall notify the Supplier of the results of such Buyer Security Tests after completion of each Buyer Security Test.

5.8. The Buyer Security Tests shall be designed and implemented so as to minimise their impact on the delivery of the Services. If a Buyer Security Test causes Supplier Non-Performance, the Buyer Security Test shall be treated as an Authority Cause for the purposes of Clause 5.1 of the Core Terms, except where the root cause of the Supplier Non-Performance was a weakness or vulnerability exposed by the Buyer Security Test.

5.9. Without prejudice to the provisions of Paragraph 5.3, where any Security Test carried out pursuant to this Paragraph 5 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Buyer of any changes to the Core Information Management System and/or the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Buyer's Approval, the 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 Buyer or, otherwise, as soon as reasonably possible.

5.10. If the Buyer unreasonably withholds its Approval to the implementation of any changes proposed by the Supplier to the Security Management Plan in accordance with Paragraph 5.9 above, the Supplier shall not be deemed to be in breach of this Call-Off Contract to the extent it can be shown that such breach:

5.10.1. has arisen as a direct result of the Buyer unreasonably withholding its Approval to the implementation of such proposed changes; and

5.10.2. would have been avoided had the Buyer given its Approval to the implementation of such proposed changes.

5.11. 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 Security Requirements and/or any obligation in this Call-Off Contract, the Supplier shall effect such change at its own cost and expense.

5.12. If any repeat Security Test carried out pursuant to Paragraph 5.3 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 Buyer may by terminate this Call-Off Contract with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 10.4 of the Core Terms.

5.13. The Supplier shall, by 31 March of each Financial Year during the Call-Off Contract Period, provide to the Buyer a letter from its chief executive officer (or equivalent officer) confirming that having made due and careful enquiry:

5.13.1. 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 Call-Off Contract; and

5.13.2. the Supplier is confident that its security and risk mitigation procedures with respect to the Services remain effective.

6. Vulnerabilities and Corrective Action

6.1. In addition to the requirements within Part B, the Supplier shall:

6.1.1. implement a mechanism for receiving, analysing and acting upon threat information supplied by NCSC, or any other competent Central Government Body;

6.1.2. promptly notify NCSC of any actual or sustained attempted Breach of Security;

6.1.3. ensure that the Core Information Management System is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

6.1.4. 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 Call-Off Contract Period;

6.1.5. pro-actively scan the Core Information Management System for vulnerable components and address discovered vulnerabilities through the processes described in the Security Management Plan;

6.1.6. from the date specified in the Accreditation Plan and within 5 Working Days of the end of each subsequent Month during the Call-Off Contract Period, provide the Buyer 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 Part B Paragraph 5.4 for applying patches to vulnerabilities in the Core Information Management System;

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

6.1.8. 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

6.1.9. inform the Buyer 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.

6.2. If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under Part B Paragraph 5.4, the Supplier shall immediately notify the Buyer.

6.3. If the Supplier fails to patch vulnerabilities in the Core Information Management System in accordance with Part B Paragraph 5.3, such failure shall constitute a material Default and the Buyer may by terminate this Call-Off Contract with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 10.4 of the Core Terms.

PART D Assurance requirements

1. This Part D sets out the Assurance arrangements the Supplier must implement before, and comply with when, providing the Services and performing its other obligations under this Call-Off Contract to ensure the security of the Government Data and the Information Management System.

1.1 The Supplier must comply with the Assurance arrangements in addition to the other Security Requirements as set out within Parts A and B and E of this Schedule and Appendix 1 (Security Management Plan).

2. **Information Security Approval Statement**

2.1 The Supplier must ensure that its Implementation Plan sets out in sufficient detail how it will ensure compliance with the requirements of this Call-Off Schedule 9 (Security Requirements), including any requirements imposed on Sub-contractors from the Call-Off Start Date.

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

2.2.1 the Supplier has procured the conduct of an ITHC of the Supplier System by a CHECK Service Provider in accordance with Paragraph 4; and

2.2.2 the Buyer has issued the Supplier with an Information Security Approval Statement in accordance with the process set out in this Paragraph 2.

2.3 The Supplier shall document in the Security Management Plan how the Supplier and its Subcontractors shall comply with the requirements set out in this Schedule and the Call-Off Contract in order to ensure the security of the Government Data and the Information Management System.

2.4 The Supplier shall prepare and submit to the Buyer within 20 Working Days of the date of this Call-Off Contract, the Security Management Plan, which comprises:

2.4.1 an Information Assurance Assessment;

2.4.2 the Required Changes Register;

2.4.3 the Personal Data Processing Statement; and

2.4.4 the Incident Management Process.

2.5 The Buyer 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:

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

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

2.6 If the Buyer rejects the Supplier's proposed Security Management Plan, the Supplier shall take the Buyer's reasons into account in the preparation of a revised Security Management Plan, which the Supplier shall submit to the Buyer for review within 10 Working Days or such other timescale as agreed with the Buyer.

2.7 The Buyer may require and the Supplier shall provide the Buyer and its authorised representatives with:

2.7.1 access to the Supplier Staff;

2.7.2 access to the Information Management System to Audit the Supplier and its Subcontractors' compliance with this Call-Off Contract;

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

2.7.4 assistance to the Buyer to establish whether the arrangements which the Supplier and its Subcontractors have implemented in order to ensure the security of the Government Data and the Information Management System are consistent with the representations in the Security Management Plan; and

2.7.5 the Supplier shall provide the access required by the Buyer 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 Buyer with the access that it requires within 24 hours of receipt of such request.

3. **Compliance Reviews**

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

3.2 The Supplier shall notify the Buyer within 2 Working Days after becoming aware of:

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

3.2.2 a new risk to the components or architecture of the Service;

3.2.3 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 5 of Part B to this Schedule;

3.2.4 a change in the threat profile;

3.2.5 a significant change to any risk component;

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

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

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

3.3 Within 10 Working Days of such notifying the Buyer or such other timescale as may be agreed with the Buyer, the Supplier shall make the necessary changes to the Required Changes Register and submit the updated Required Changes Register the Buyer for review and Approval.

3.4 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.

4. **Security Testing**

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

4.1.1 testing of the Information Management System by a CHECK Service Provider ("**ITHC**"); and

4.1.2 such other security tests as may be required by the Buyer; and

4.1.3 the Supplier shall complete all of the above security tests before the Supplier submits the Security Management Plan to the Buyer for review in accordance with Paragraph 3; and it shall repeat the ITHC not less than once every 12

Months during the Term and submit the results of each such test to the Buyer for review in accordance with this Paragraph.

4.2 In relation to each ITHC, the Supplier shall:

4.2.1 agree with the Buyer the aim and scope of the ITHC;

4.2.2 promptly, and no later than 10 Working Days, following the receipt of each ITHC report, provide the Buyer with a copy of the full report;

4.2.3 in the event that the IT Health Check report identifies any vulnerabilities, the Supplier shall:

(a) prepare a remedial plan for Approval by the Buyer (each a "**Vulnerability Correction Plan**") which sets out in respect of each vulnerability identified in the ITHC report:

(i) how the vulnerability will be remedied;

(ii) the date by which the vulnerability will be remedied; and

(iii) the tests which the Supplier shall perform or procure to be performed (which may, at the discretion of the Buyer, include a further IT Health Check) to confirm that the vulnerability has been remedied;

(b) comply with the Vulnerability Correction Plan; and

(c) conduct such further tests on the Service as are required by the Vulnerability Correction Plan to confirm that the Vulnerability Correction Plan has been complied with.

4.3 The Supplier shall ensure that any testing which could adversely affect the Supplier System shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such tests shall be agreed in advance with the Buyer.

4.4 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 days of becoming aware of such risk, threat, vulnerability or exploitation technique provide the Buyer with a copy of the test report and:

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

4.4.2 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 Buyer.

4.5 The Supplier shall conduct such further tests of the Supplier System as may be required by the Buyer from time to time to demonstrate compliance with its obligations set out this Schedule and the Call-Off Contract.

4.6 The Supplier shall notify the Buyer immediately if it fails to, or believes that it will not, mitigate the vulnerability within the timescales set out in Paragraph 5 of Part B to this Schedule.

Part E Certification requirements

Certification Requirements

1. Supplier Requirements

1.1. The Supplier shall as applicable to the Lot and the associated Security Tier, ensure, at all times during the Call-Off Contract Period, that it is certified as compliant with:

1.1.1. ISO/IEC 27001:2013 by a UKAS approved certification body or are included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; and

1.1.2. Cyber Essentials or Cyber Essentials PLUS as applicable to the Lot and Security Tier of the Service, in accordance with the requirements in Framework Schedule 9 (Cyber Essentials Scheme), and shall provide the Buyer with a copy of each such certificate of compliance before the Supplier or the relevant Subcontractor (as applicable) shall be permitted to use the Core Information Management System to receive, store or Process any Government Data.

2. **Payment Card Industry Data Security Standard (PCI DSS) Compliance**

2.1. All Suppliers and / or Subcontractors that are a payment processor must be, and remain, appropriately certified according to the Payment Card Industry Data Security Standard requirements throughout the term of the Contract

2.2. Where the Supplier and / or Subcontractor intends to accept payments, restricted to at sale only, by debit/credit card the Supplier and / or Subcontractor must have either:

2.2.1. been certified by a Qualified Security Assessor as being compliant with the PCI DSS version 1.1;

2.2.2. completed an internal self-assessment and will adhere at all times to the terms of the PCI DSS and will notify the Client promptly in writing of any changes in the Contractor's certification.

2.3. The Supplier / Subcontractor must validate compliance in the manner deemed appropriate by the card scheme industry on an annual basis and provide the Buyer with written evidence of compliance annually.

2.4. The Supplier / Subcontractor will be responsible for any costs incurred to attain and maintain compliance with PCI DSS.

2.5. The Supplier / Subcontractor must meet all PCI DSS requirements, on a continuing basis, including but not limited to any subsequent versions of the PCI DSS.

2.6. The Supplier / Subcontractor must be responsible for the security of all cardholder Data in their possession and must protect data by the card scheme industry standard on an

annual basis and provide the Buyer access hosted environment and data when necessary.

2.7. The Supplier / Subcontractor must notify the Buyer and the card scheme industry immediately if it knows or suspects that there has been, or will be, a breach of the security of Cardholder Data or of the PCI DSS.

2.8. The Supplier / Subcontractor must indemnify the Buyer, its subsidiaries, affiliates, officers, employees and agents from and against all actions, demands, costs, Losses, whatsoever incurred by it or them arising out of or in connection with the Supplier's non-compliance with, or breach of, the PCI DSS or breach of Cardholder Data security.

2.9. The Supplier / Subcontractor must cease taking payments, by Debit Card / Credit Card, on behalf of the Buyer in the event that the Supplier becomes non-compliant with, or suffers a breach of, the PCI DSS or breach of Cardholder Data security.

3. **Subcontractor Requirement**

3.1. Notwithstanding anything else in this Contract, a CMIS Subcontractor shall be treated for all purposes as a Key Subcontractor.

3.2. In addition to the obligations contained in Joint Schedule 6 (Key Subcontractors), the Supplier must ensure that the Key Subcontract with each CIMS Subcontractor.

3.3. contains obligations no less onerous on the Key Subcontractor than those imposed on the Supplier under this Call-Off Schedule 9 (Security Requirements);

3.3.1. provides for the Buyer to perform Accreditation of any part of the Core Information Management System that the CIMS Subcontractor provides or operates which is not otherwise subject to Accreditation under this Call-Off Schedule 6 (Security Requirements).

3.4. The Supplier shall ensure that each Higher Risk Subcontractor is certified as compliant, and the Supplier shall provide the Buyer with a copy of each such certificate of compliance before the Higher-Risk Subcontractor shall be permitted to receive, store or Process Government Data, with either:

3.4.1. ISO/IEC 27001:2013 by a United Kingdom Accreditation Service-approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; or

3.4.2. Cyber Essentials PLUS, in accordance with the requirements in Framework Schedule 9 (Cyber Essentials Scheme),

3.5. The Supplier shall ensure that each Medium Risk Subcontractor is certified compliant with Cyber Essentials, in accordance with the requirements in Framework Schedule 9 (Cyber Essentials Scheme).

3.6. The Supplier shall notify the Buyer as soon as reasonably practicable and, in any event within 2 Working Days, if the Supplier or any Subcontractor ceases to be compliant with the Certification Requirements and, on request from the Buyer, shall or shall procure that the relevant Subcontractor shall:

3.6.1. immediately ceases using the Government Data; and

3.6.2. procure that the relevant Subcontractor promptly returns, destroys and/or erases the Government Data in accordance with Security Requirements.

3.7. The Buyer may agree to exempt, in whole or part, the Supplier or any Subcontractor from the Certification Requirements. Any exemption must be in writing to be effective. The Supplier must include the exemption in the Security Management Plan.

Call Off Schedule 9 (Security Requirements)
Call Off Ref: [Redacted]

Appendix 1

Security Management Plan Template

[Guidance Note: This template shall be completed by the Supplier in accordance with the applicable Tier of Security Requirements for the particular Lots awarded]

DRS Call-Off Schedule 9 (Appendix 1)

Security Management Plan Template

[Lot/Service]

[Supplier Name]

Author:

Owner:

Date:

Version:

Call Off Schedule 9 (Security Requirements)
Call Off Ref: [Redacted]

[Guidance Note: ***The Supplier shall complete this Security Management Plan Template in as much detail as possible and if any provision does not apply to the Supplier, it must explain why.*****]**

1 Executive Summary

<This section should contain a brief summary of the business context of the Supplier System [including any Subcontractor system], any key Information Assurance controls, assurance work done, off-shoring considerations and significant residual risks that need acceptance by the Buyer.>

Call Off Schedule 9 (Security Requirements)
Call Off Ref: [Redacted]

1.1 List of Contents

1.1 Security Requirements Change History

Version Number	Date of Change	Change made by	Nature and reason for change

1.2 References, Links and Dependencies

This Security Management Plan Template relies upon the supporting information and assurance provided by the following documents:

ID	Document Title	Reference	Date
1.			
2.			
3.			

2 System Description

3 Background

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

4 Organisational Ownership/Structure

< Who owns the system, 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 Buyer and Buyer governance *board as per their Call-Off Contract.>*

5 Information assets and flows

<The information assets processed by the system, which should include a simple high level diagram on one page, as well as a list of the type and volumes of data that will be processed, managed and stored within the Supplier System. If Personal Data is processed, please include the fields used such as name, address, department DOB, NI number etc. in Annex 1 of Joint Schedule 11 (Processing Data).>

6 System Architecture

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

7 Users

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

8 Locations

<Detail where the data assets are stored and managed from. If any locations hold independent security certifications (e.g. ISO27001:2013) these should be specified, as well as any off-shoring considerations.>

9 Test and Development Systems

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

10 Key roles and responsibilities

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

11 Accreditation/Assurance Scope

<This section should describe the scope of the Accreditation/Assurance for the system (applicable to Tier 1 and Tier 2 Security Requirements). The scope of the assurance assessment should be clearly indicated, expressly including those components upon which reliance is placed but where assurance will not be undertaken, e.g. a cloud hosting service. A logical diagram should be inserted here along with a brief description of the components.>

12 Risk appetite

<A risk appetite should be agreed with the Buyer's Head of IA and detailed here.>

13 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 could make HMG liable to an Information Commissioner Office investigation) 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.>

14 Risk assessment

<The content of this section will depend on the risk assessment methodology chosen. It should contain a prioritised list of the output of the formal information risk using plain English 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

15 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 ISO27001 certification

16 Residual risks and actions

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

17 In-service controls

< This section should describe the controls relating to the information lifecycle, including development, testing, in-service, termination and on-going risk management and accreditation assurance. Details of any formal assurance requirements specified in the Contract such as security CHECK testing or maintained ISO27001 certification should be included. This section should include as a minimum:

a) *information risk management and timescales and triggers for a review;*

b) *contractual patching requirements and timescales for the different priorities of patch;*

c) *protective monitoring arrangements to include how anomalous behaviour is identified and acted upon as well as how logging and auditing of user activity is done;*

d) *configuration and change management;*

e) *incident management;*

f) *vulnerability management;*

g) *user access management; and*

h) *data sanitisation and disposal.>*

18 Security Operating Procedures (SyOPs)

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

19 Third Party Subcontractors/Suppliers/Products

< Please provide a table of any third party subcontractor/suppliers and products that you are using to deliver your Services for the Buyer. Please also include the location of where they are Processing or storing the Data and what function they are performing as well as how they comply with the contractual security requirements. >

20 Physical Security

<Please provide details of the building where the service will operate from and describe the procedures and security in place to control access to premises and any areas holding Buyer assets. Detail the measures such as construction of buildings used for handling Buyer assets, availability of lockable storage, procedures covering end of day/silent hours, key management, visitor controls. Also include details of any automated access controls, alarms and CCTV coverage and details of the maintenance schedule of these security controls.>

21 Major Hardware and Software and end of support dates

< Please complete a table listing the end of support dates for hardware and software products and components. For example:>

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

22 Incident Management Process

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

23 Security Requirements for User Organisations

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

24 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.	Buyer's name	11/11/2018	Jul-2019	Open

25 Personal Data Processing Statement

<The Supplier shall complete Annex 1 of Joint Schedule 11 (Processing Data) detailing: (i) the types of Personal Data which the Supplier and/or its Subcontractors are Processing on behalf of the Buyer; (ii) the categories of Data Subjects whose Personal Data the Supplier and/or its Subcontractors are Processing on behalf of the Buyer; (iii) the nature and purpose of such Processing; (iv) the locations at which the Supplier and/or its Subcontractors

Process Buyer Data; and, (v) the Protective Measures that the Supplier and, where applicable, its Subcontractors have implemented to protect the Buyer Data against a Security Breach including a Personal Data Breach.>

-:-

26 Annex A: ISO27001 and/or Cyber Essential Plus certificates

<Any certifications relied upon should have their certificates included>

27 Annex B: Cloud Security Principles assessment

<A spreadsheet may be attached>

28 Annex C: Protecting Bulk Data assessment if required by the Buyer

<A spreadsheet may be attached>

29 Annex D: Latest ITHC report and Vulnerability Correction Plan

Appendix 2

ACCREDITATION - CORE INFORMATION MANAGEMENT SYSTEM DIAGRAM

Not Used

Appendix 3

BUYER SECURITY POLICIES AND STANDARDS

The Security Policies are published on:

https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards unless specified otherwise:

a) Acceptable Use Policy

b) Information Security Policy

c) Personnel Security Policy

d) Physical Security Policy

e) Information Management Policy

f) Email Policy

g) Technical Vulnerability Management Policy

h) Remote Working Policy

i) Social Media Policy

j) Forensic Readiness Policy

k) Microsoft Teams recording and transcription policy

l) SMS Text Policy

m) Privileged Users Security Policy

n) Protective Monitoring Security Policy

o) User Access Control Policy

p) Security Classification Policy

q) Cryptographic Key Management Policy

r) HMG Personnel Security Controls – May 2018
(published on https://www.gov.uk/government/publications/hmg-personnel-security-controls)

s) NCSC Secure Sanitisation of Storage Media (published on https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media)

Appendix 4

SECURITY STANDARDS

The Security Standards are published on:

https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards:

a) SS-001 - Part 1 - Access & Authentication Controls
b) SS-001 - Part 2 - Privileged User Access Controls
c) Security Standard Physical and Electronic Security (Part 1)
d) SS-002 - PKI & Key Management
e) SS-003 - Software Development
f) SS-005 - Database Management System
g) SS-006 - Security Boundaries
h) SS-007 - Use of Cryptography
i) SS-008 - Server Operating System
j) SS-009 - Hypervisor
k) SS-010 - Desktop Operating System
l) SS-011 - Containerisation
m) SS-012 - Protective Monitoring Standard for External Use
n) SS-013 - Firewall Security
o) SS-014 - Security Incident Management
p) SS-015 - Malware Protection
q) SS-016 - Remote Access

r) SS-017 - Mobile Devices
s) SS-018 - Network Security Design
t) SS-019 - Wireless Network
u) SS-022 - Voice & Video Communications
v) SS-023 - Cloud Computing
w) SS-025 - Virtualisation
x) SS-027 - Application Security Testing
y) SS-028 - Microservices Architecture
z) SS-029 - Securely Serving Web Content
aa) SS-030 - Oracle Database
bb) SS-031 - Domain Management
cc) SS-033 – Security Patching
dd) SS-035 – Backup and Recovery
ee) SS-036 – Secure Sanitisation and Destruction

Appendix 5
Information Security Questionnaire Template

[Redacted].