CPS PRINT SERVICES

CALL OFF SCHEDULE 7: SECURITY

CALL OFF SCHEDULE 7: SECURITY

1. DEFINITIONS

1.1 In this Call Off Schedule 7 the following words shall have the following meanings and they shall supplement Call Off Schedule 1 (Definitions):

"**Accreditation / Assurance Strategy**"	means the Customer's Assurance Strategy set out in Annex 3 to this Call Off Schedule 7;
"**Assurance Authority**"	means the CPS security individual who will ensure acceptance of the completed Supplier Assurance Statement. At the Call Off Commencement Date, this is Roger Sutton (Head of CPS Cyber Security);
"**Breach(es) of Security**"	means the occurrence of: a) any unauthorised access to or use of the Deliverables, the Sites and/or any Information and Communication Technology ("**ICT**"), information or data (including the Confidential Information and the Government Data) used by the Customer and/or the Supplier in connection with this Call Off Contract; and/or b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Customer and/or the Supplier in connection with this Call Off Contract, (in either case) as set out in the security requirements in the Security Policy;
"**ISMS**"	the information security management system and process developed by the Supplier in accordance with paragraph 4 of this Call Off Schedule 7 as updated from time to time in accordance with this Call Off Schedule 7;
"**National Minimum Cyber Security Standard**"	means as referenced in Annex 1 and any subsequent updates;
"**Security Tests**"	tests to validate the ISMS and security of all relevant processes, systems, incident response plans, patches to vulnerabilities and mitigations to Breaches of Security; and
"Supplier Assurance Statement"	the statement of compliance made by the Supplier in accordance with paragraph 5.2.2 of this Call Off Schedule 7.

2. OVERVIEW

The Parties acknowledge that the purpose of the ISMS and Security Management Plan are to ensure an effective approach to security under which the specific requirements of this Call Off Contract will be met. This approach should ensure compliance with the Customer's obligations in relation to the Security Policy Framework and all subordinate and associated best practice policies and guidance and also support wider security requirements such as those required for access to externally provisioned shared and assured services (e.g. compliance with conditions for connection). The approach should also support all Customer's legislative compliance obligations with an emphasis on the security specific aspects of Data Protection Legislation.

3. INTRODUCTION

3.1 The Customer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), CCS shall have the right to enforce the Customer's rights under this Call Off Schedule 7.

3.2 The Parties shall each appoint named individuals to be responsible for security in connection with this Call Off Contract. The initial security representatives of the Parties are:

3.2.1 The CPS claims an exemption from publishing this information under Section 40(2) of the FOI Act 2000 ; and

3.2.2 and the provisions of Call Off Schedule 4 (Implementation Plan, Customer Responsibilities, Key Personnel and Sub-Contractors) of the Call Off Contract shall apply in relation to such person.

3.3 The Customer shall articulate its high level security requirements driven by the sensitivity of Customer Data which shall be identified at the Government Security Classification of 'OFFICIAL' so that the Supplier can ensure that the ISMS, security related activities and any mitigations are driven by these fundamental needs. It should be noted that casework data is identified as 'OFFICIAL-SENSITIVE' and the Supplier shall apply any necessary additional controls that are required to handle.

3.4 Each Party shall provide a reasonable level of access to any members of its Customer personnel or Supplier Personnel (as applicable) and to any premises as required for the purposes of designing, implementing and managing security.

3.5 The Supplier shall use as a minimum Good Industry Practice in the day to day operation of any system holding, transferring or processing Customer Data and any system that could directly or indirectly have an impact on that information, and shall ensure that the Customer Data remains under the effective control of the Supplier at all times

3.6 The Supplier shall ensure the up-to-date maintenance of a security policy relating to the operation of its own organisation and systems and on request shall supply evidence of this (e.g. appropriately scoped ISO/IEC 27001 registration/certificate) as soon as practicable to the Customer.

3.7 The Supplier shall comply with the following security principles and requirements where access to Sites (including Home Worker Sites) is required:

3.7.1 the Supplier Personnel carrying out the Services on Site must be SC cleared as a minimum. For each Supplier Personnel carrying out the Services on Site

the Supplier shall provide to the Customer's security team at the following email address:

The CPS claims an exemption from publishing this information under Section 43(1) of the FOI Act 2000

the required clearance paperwork together with the Supplier Personnel's full name and date of birth. Such details shall be provided at least five (5) Working Days before any scheduled visit to allow the Customer to check the information against the UKSV clearance system and to ensure that clearance is up to date and valid. Approval to access site will be provided within 48 hours of the required information being provided or, if earlier, as soon as clearance has been confirmed;

3.7.2 the Supplier shall ensure that the Customer's Facilities Estate Security Manager (FESM) is informed of each visit (including the proposed date and time of each visit) a minimum of five (5) Working Days' in advance. The Customer's FESM will, where required, provide an accompanying person for the Supplier Personnel visit to Site; and

3.7.3 the Supplier Personnel carrying out the Services on Site shall, at all times whilst on the Sites, display their Supplier provided personal identification and carry any passport held.

3.8 The Supplier shall complete and maintain Cyber Essentials certification.

3.9 The Customer and the Supplier acknowledge that a compromise of either the Supplier or the Customer's security provisions represents an unacceptable risk to the Customer, requiring immediate communication and co-operation between the Parties.

4. INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

4.1 By the date specified in the Implementation Plan, the Supplier shall develop and submit to the Customer for Approval in accordance with paragraph 4.6 of this Call Off Schedule 7, an ISMS (Information Security Management System) for the purposes of this Call Off Contract, which shall:

4.1.1 have been tested in accordance with this Call Off Schedule 7; and

4.1.2 comply with the requirements of paragraphs 4.3 to 4.5 of this Call Off Schedule 7.

4.2 The Supplier acknowledges that the Customer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on the security provided by the ISMS and that the Supplier shall be responsible for the effective performance of the ISMS.

4.3 The ISMS shall:

4.3.1 unless otherwise specified by the Customer in writing, be developed to protect all aspects of the Services and all processes associated with the delivery of the Services, including the Customer Premises, the Sites, the Supplier System, the Customer System (to the extent that it is under the control of the Supplier),

connectivity to secure services (e.g. PSN) and any IT, information and data (including Sensitive Information and the Customer Data) to the extent used by the Customer or the Supplier in connection with this Call Off Contract;

4.3.2 achieve certification to the extant version of ISO/IEC 27001 within a timescale agreed by the Customer and in accordance with paragraph 8 of this Call Off Schedule 7;

4.3.3 be confirmed to be 'fit for purpose' from a security and assurance perspective by the Customer acting as Assurance Authority. This will be achieved by the Supplier complying with the Customer's Accreditation / Assurance Strategy and associated approach and only achieved following the production of specified assurance documentation to a standard deemed acceptable by the Customer;

4.3.4 comply with any other relevant mutually agreed security standard that may be appropriate to the proposed Services, solution or technology arrangement as identified by the Customer from time to time;

4.3.5 at all times provide a level of security which:

(a) is in accordance with Law and this Call Off Contract;

(b) demonstrates Good Industry Practice;

(c) complies with extant national security and criminal justice specific obligations and National Minimum Cyber Security Standards, ensuring all accreditation and secure connectivity objectives are fulfilled;

(d) complies with the requirements referred to in Annex 2 of this Call Off Schedule 7;

(e) addresses issues of incompatibility with the Supplier's own organisational security policies;

(f) meets any specific security threats of immediate relevance to the Services and/or Customer Data;

(g) complies with the operational security requirements as set out in Call Off Schedule 2 (Requirements); and

(h) comply with the Customer security PPPs as notified to the Supplier in writing;

(i) document the security incident management processes and incident response plans and cooperate with the Customer and/or its nominated agent to deliver an integrated incident management process;

(j) document the vulnerability management policy including processes for identification of system vulnerabilities and assessment of the potential impact on the Services of any new threat, vulnerability or exploitation technique, prioritisation of security patches, testing of security patches, application of security patches, a process for Customer Approvals of exceptions, and the reporting and audit mechanism detailing the efficacy of the patching policy;

(k) be certified by (or by a person with the direct delegated authority of) a Supplier's main board representative, being the Chief Security Officer, Chief Information Officer, Chief Technical Officer or Chief Financial Officer (or equivalent as agreed in writing by the Customer in advance of issue of the relevant Security Management Plan); and

(l) be supported by the Supplier's attendance of scheduled and ad-hoc security working group meetings as determined by the Customer.

4.4 All references to standards, guidance and policies set out in paragraph 4.3 of this Call Off Schedule 7 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time. Where reference is made to the Security Policy Framework, the Supplier shall take account of the range of policy and guidance information that has been drafted by organisations such as Cabinet Office and the National Cyber Security Centre to support compliance with this framework.

4.5 In the event that the Supplier becomes aware of any inconsistency in the provisions of the standards, guidance and policies set out in paragraph 4.3 of this Call Off Schedule 7, the Supplier shall immediately notify the Customer Representative of such inconsistency and the Customer Representative shall, as soon as practicable, notify the Supplier which provision the Supplier shall comply with.

4.6 If the ISMS submitted to the Customer pursuant to paragraph 4.1 of this Call Off Schedule 7 is Approved by the Customer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Call Off Schedule 7. If the ISMS submitted to the Customer pursuant to paragraph 4.1 of this Call Off Schedule 7 is not Approved by the Customer, the Customer will serve a notice of non-Approval, providing details of its concerns and reasoning for non-Approval of the ISMS, and the Supplier shall within ten (10) Working Days of the Customer's notice of non-Approval amend the ISMS and re-submit it to the Customer for Approval. Any related technical work to be implemented by the Supplier shall be agreed in accordance with Call Off Schedule 12 (Change Control Procedure). The Parties shall use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Customer. If the Customer does not Approve the ISMS following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Customer pursuant to this paragraph 4 of this Call Off Schedule 7 may be unreasonably withheld or delayed. However any failure to Approve the ISMS on the grounds that it does not comply with any of the requirements set out in paragraphs 4.3 to 4.5 of this Call Off Schedule 7 shall be deemed to be reasonable.

4.7 Approval by the Customer of the ISMS pursuant to paragraph 4.6 of this Call Off Schedule 7 or of any change to the ISMS shall not relieve the Supplier of its obligations under this Call Off Schedule 7.

5. SECURITY MANAGEMENT PLAN

5.1 Within forty (40) Working Days after the Call Off Commencement Date, the Supplier shall prepare and submit to the Customer for Approval in accordance with paragraph 5.3 of this Call Off Schedule 7 fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of paragraph 5.2 of this Call Off Schedule 7.

5.2 The Security Management Plan shall:

5.2.1 be based on the initial Security Management Plan that will have been provided by the Supplier as part of the original Tender response;

5.2.2 incorporate the approved Supplier Assurance Statement for Print Services in accordance with the tab titled "Supplier Assurance Statement" in the Accreditation / Assurance Strategy, as set out in Annex 3 to this Call Off Schedule 7;

5.2.3 comply with any National Minimum Cyber Security Standards, and the requirements referred to in Annex 2 of this Call Off Schedule 7, and support compliance with organisational and government Security Policy obligations;

5.2.4 confirm how the security controls contained within Call Off Schedule 2 (Requirements) are met;

5.2.5 identify the necessary delegated organisational roles defined for those responsible for ensuring this Call Off Schedule 7 is complied with by the Supplier;

5.2.6 detail the process for managing any security risks from Sub-Contractors and third parties authorised by the Customer with access to the Services, processes associated with the delivery of the Services, the Customer Premises, the Sites, the Supplier System, the Customer System (to extent that it is under the control of the Supplier) and any IT, information and data (including Sensitive Information and the Customer Data) and any system that could directly or indirectly have an impact on that information, data and/or the Services;

5.2.7 unless otherwise specified by the Customer in writing, be developed to protect all aspects of the Services and all processes associated with the delivery of the Services, including the Customer Premises, the Sites, Supplier's Sites, the Supplier System, the Customer System (to the extent that it is under the control of the Supplier) and any IT, information and data (including Sensitive Information and the Customer Data) to the extent used by the Customer 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;

5.2.8 set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Services and all processes associated with the delivery of the Services and at all times comply with and specify security measures and procedures which are sufficient to ensure that the Services comply with the provisions of this Call Off Schedule 7(including the requirements set out in paragraph 4.3 of this Call Off Schedule 7);

5.2.9 demonstrate that the Supplier Solution has minimised the Customer and Supplier effort required to comply with this Call Off Schedule 7 through consideration of available, appropriate and practicable pan-government accredited / approved or pre-assured services;

5.2.10 set out the plans for transiting all security arrangements and responsibilities from those in place at the Call Off Commencement Date to those incorporated in the ISMS by the date set out in Call Off Schedule 4 (Implementation Plan,

Customer Responsibilities, Key Personnel and Sub-Contractors) for the Supplier to meet the full obligations of the security requirements set out in Call Off Schedule 2 (Requirements) and this Call Off Schedule 7;

5.2.11 set out the scope of the Customer System that is under the control of the Supplier;

5.2.12 be structured in accordance with ISO/IEC 27001 and ISO/IEC 27002, cross-referencing if necessary to other Call Off Schedules which cover specific areas included within those standards (e.g. business continuity management/DR); and

5.2.13 be written in plain language which is readily comprehensible to the staff of the respective Parties engaged in the Services and shall reference only documents which are in the possession of the Parties or whose location is otherwise specified in this Call Off Schedule 7.

5.3 If the Security Management Plan submitted to the Customer pursuant to paragraph 5.1 of this Call Off Schedule 7 is:

5.3.1 Approved by the Customer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Call Off Schedule 7;

5.3.2 not Approved by the Customer, the Customer will serve a notice of non-Approval, providing details of its concerns and reasoning for non-Approval of the Security Management Plan, and the Supplier shall within ten (10) Working Days of the Customer's notice of non-Approval amend the Security Management Plan and re-submit it to the Customer for Approval.

5.4 Any related technical work to be implemented by the Supplier shall be agreed in accordance with Call Off Schedule 12 (Change Control Procedure). The Parties shall use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Customer.

5.5 If the Customer does not Approve the Security Management Plan following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Customer pursuant to this paragraph 5.5 of this Call Off Schedule 7 may be unreasonably withheld or delayed. However any failure to Approve the Security Management Plan on the grounds that it does not comply with the requirements set out in paragraph 5.2 of this Call Off Schedule 7 shall be deemed to be reasonable.

5.6 Approval by the Customer of the Security Management Plan pursuant to paragraph 5.3 of this Call Off Schedule 7 or of any change or amendment to the Security Management Plan shall not relieve the Supplier of its obligations under this Call Off Schedule 7.

6. AMENDMENT AND REVISION OF THE ISMS AND SECURITY MANAGEMENT PLAN

6.1 The ISMS and Security Management Plan shall be fully reviewed and updated by the Supplier at least annually to reflect:

6.1.1 emerging changes in Good Industry Practice and changes to Government security policy and guidance;

6.1.2 on-going ISO/IEC 27001 certification requirements;

6.1.3 on-going Customer Accreditation / Assurance Strategy and obligations;

6.1.4 any change or proposed change to the Customer System, Supplier System, the Services and/or associated processes;

6.1.5 any new perceived or changed security threats; and

6.1.6 any reasonable change in requirements requested by the Customer.

6.2 The Supplier shall provide the Customer with the results of such reviews as soon as reasonably practicable after their completion and amend the ISMS and Security Management Plan at no additional cost to the Customer. The results of the review shall include, without limitation:

6.2.1 suggested improvements to the effectiveness of the ISMS (e.g. corrective actions identified by an external accredited certification body);

6.2.2 updates to the risk assessments;

6.2.3 proposed modifications to respond to events that may impact on the ISMS including the security incident management process, incident response plans and general procedures and controls that affect information security; and

6.2.4 suggested improvements in measuring the effectiveness of controls and improved performance measures and targets (e.g. *x*% reduction in incidents in the next 12 Months).

6.3 Subject to Clause 34 of the Call Off Terms and paragraph 6.4 of this Call Off Schedule 7, any change which the Supplier proposes to make to the ISMS or Security Management Plan (as a result of a review carried out pursuant to paragraph 6.1 of this Call Off Schedule 7, a Customer request, a Change to Call Off Schedule 2 (Requirements), or otherwise) shall be subject to the Change Control Procedure detailed in Call Off Schedule 12 (Change Control Procedure) and shall not be implemented until Approved in writing by the Customer.

6.4 The Customer may, where it is reasonable to do so, Approve and require changes or amendments to the ISMS or Security Management Plan to be implemented on timescales faster than set out in the Change Control Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Change Control Procedure for the purposes of formalising and documenting the relevant change or amendment for the purposes of this Call Off Contract.

7. SECURITY TESTING

7.1 The Supplier shall conduct Security Tests from time to time (and at least annually across the scope of the ISMS) and additionally after any change or amendment to the

ISMS (including security incident management processes and incident response plans) or the Security Management Plan. Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Deliverables and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Customer. Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests.

7.2 The Customer shall be entitled to send a representative to witness the conduct of the Security Tests. The Supplier shall provide the Customer with the results of such Security Tests (in a form approved by the Customer in advance) as soon as practicable after completion of each Security Test.

7.3 Without prejudice to any other right of audit or access granted to the Customer pursuant to this Call Off Contract, the Customer and/or its authorised representatives shall be entitled, at its own cost, at any time upon giving reasonable notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the Supplier's compliance with the ISMS and the Security Management Plan. The Customer may notify the Supplier of the results of such tests after completion of each such test. Any penetration testing carried out under this paragraph 7.3 shall only be undertaken by an approved service provider from the then-current NCSC list (https://www.ncsc.gov.uk/scheme/penetration-testing).

7.4 Where any Security Test carried out pursuant to paragraphs 7.2 or 7.3 of this Call Off Schedule 7 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 Customer of any changes to the ISMS and to 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 Customer's prior written Approval, the Supplier shall implement such changes to the ISMS and the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Customer or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan is to address a non-compliance with the Security Policy or security requirements (as set out in Annex 1 (National Minimum Cyber Security Standard) to this Call Off Schedule 7) or the requirements of this Call Off Schedule 7, the change to the ISMS or Security Management Plan shall be at no cost to the Customer.

7.5 If any repeat Security Test carried out pursuant to paragraph 7.3 of this Call Off Schedule 7 reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall constitute a material Default of this Call Off Contract.

7.6 At its own cost, the Supplier shall carry out penetration testing at least annually to check the Supplier's compliance with the ISMS and the Security Management Plan. Such penetration testing shall only be undertaken by an approved service provider from the then-current NCSC list (https://www.ncsc.gov.uk/scheme/penetration-testing). This testing shall directly support Customer Accreditation / Assurance requirements and be undertaken at least annually in support of these requirements.

8. COMPLYING WITH THE ISMS

8.1 The Customer shall be entitled to carry out such security audits as it may reasonably deem necessary in order to ensure that the ISMS maintains compliance with all Security Policy and system accreditation/assurance objectives including under the Customer Accreditation / Assurance Strategy, and the specific security requirements set out or referred to:

8.1.1 elsewhere in this Call Off Schedule 7;

8.1.2 in Call Off Schedule 2 (Requirements); and/or

8.1.3 in the National Minimum Cyber Security Standards.

8.2 The Customer shall be entitled to carry out such security audits as it may reasonably deem necessary in order to ensure that the ISMS maintains compliance.

8.3 ISO/IEC 27001 certification/registration shall be confirmed by an external accredited certification body on an annual basis at the cost of the Supplier.

8.4 If, on the basis of evidence provided by such audits, it is the Customer's reasonable opinion that compliance with identified security principles and practices, the specific security requirements set out or referred to in the Call Off Schedules and standards listed in paragraph 8.1 of this Call Off Schedule 7 is not being achieved by the Supplier, then the Customer shall notify the Supplier of the same and give the Supplier a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to implement any necessary remedy. If the Supplier does not become compliant within the required time then the Customer shall have the right to obtain an independent audit against these standards in whole or in part.

8.5 If, as a result of any such independent audit as described in paragraph 7.3 of this Call Off Schedule 7 the Supplier is found to be in material Default of the identified security principles and practices, the specific security requirements set out or referred to in the Call Off Schedules and standards listed in paragraph 8.1 of this Call Off Schedule 7 then the Supplier shall, at its own expense, undertake those actions required in order to achieve the necessary compliance shall reimburse the Customer for all reasonable costs incurred by the Customer in the course of the audit.

9. BREACH OF SECURITY AND PERSONAL DATA BREACHES

9.1 Either Party shall notify the other in accordance with the agreed security incident management process as defined by the ISMS upon becoming aware of any Breach of Security or attempted Breach of Security.

9.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in paragraph 9.1 of this Call Off Schedule 7, the Supplier shall:

9.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Customer) necessary to:

9.2.2 minimise the extent of actual or potential harm caused by any Breach of Security;

9.2.3 remedy such Breach of Security to the extent possible and protect the integrity of the Services technical environment to the extent within its control against any such Breach of Security or attempted Breach of Security;

9.2.4 providing that reasonable testing has been undertaken by the Supplier, apply a mitigation against any such Breach of Security or attempted Breach of Security. If the mitigation adversely affects the Supplier's ability to deliver the Services so as to meet the Service Levels, the Supplier shall be granted relief against any resultant under-performance for such period as the Customer, acting reasonably, may specify by written notice to the Supplier;

9.2.5 prevent a further Breach of Security or attempted Breach of Security in the future exploiting the same Root Cause failure;

9.2.6 supply any requested data to the Customer or the National Cyber Security Centre (NCSC) on the Customer's request within three (3) Working Days and without charge (where such requests are reasonably related to a possible incident or compromise); and

9.2.7 as soon as reasonably practicable, and in any event within thirty (30) minutes of identification provide to the Customer full details (using the reporting mechanism defined by the ISMS) of the Breach of Security or attempted Breach of Security, to be followed up by a Root Cause analysis where required by the Customer, within five (5) Working Days of the Incident.

9.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the ISMS with the National Minimum Cyber Security Standard or security requirements set out or referred to in Call Off Schedule 2 (Requirements), and this Call Off Schedule 7, or the Breach of Security results from any non-compliance with this Call Off Schedule 7, then any required change to the ISMS shall be at no cost to the Customer.

9.4 Either Party becoming aware of a Personal Data Breach affecting the other Party's data protection responsibilities shall notify the other Party. The Supplier shall ensure that the Customer Representative is notified without undue delay in accordance with the requirements of paragraph 1.6 of Call Off Schedule 17 (Data Processing) and, in parallel, the Supplier shall also notify the Customer's Service Desk supplier of any Personal Data Breach in order to fulfil its obligations under Major Incident procedures and, as appropriate, the Other Suppliers should the Personal Data Breach impact upon their ability to deliver their services or significantly increase risk in the Customer's ICT Environment.

10. VULNERABILITIES AND FIXING THEM

10.1 The severity of threat vulnerabilities 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 ISMS and using the appropriate vulnerability scoring systems including:

10.1.1 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 http://nvd.nist.gov/cvss.cfm);

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

10.1.3 any other centralised source of vulnerability information directly relating to technology deployed within the solution.

The Supplier shall revise promptly any categorisation that it makes pursuant to this paragraph 10.1 of this Call Off Schedule 7 as requested by the Customer from time to time.

10.2 Subject to Approval from the Customer, the Supplier shall procure the application of security patches (including public release patches) to vulnerabilities categorised as 'Critical' within four (4) hours of such Approval, 'Important' within ten (10) Working Days of Approval and all 'Other' within forty (40) Working Days of Approval, except where:

10.2.1 the Supplier can demonstrate that a vulnerability is not exploitable within the context of any Service (e.g. because it resides in a Component of the Software which is not running in the service) provided vulnerabilities which the Supplier asserts cannot be exploited within the context of a Service must be remedied by the Supplier within the above timescales if the vulnerability becomes exploitable within the context of the Service;

10.2.2 the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services in which case the Customer may (in its absolute discretion) grant the Supplier an extension to such timescales , provided the Supplier had followed and continues to follow the security patch test plan agreed with the Customer;

10.2.3 the Customer agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the ISMS; or

10.2.4 the relevant information technology vendor recommends the application of security patches to vulnerabilities within a shorter time period in which case the patches will be applied in accordance with the vendor's recommendations.

10.3 Where any of the exceptions identified within paragraphs 9.2.1 to 9.2.7 of this Call Off Schedule 7 apply, the Supplier shall apply patches in accordance with the defined requirements outlined for Cyber Essentials - https://www.cyberessentials.ncsc.gov.uk/requirements-for-it-infrastructure

10.4 The Supplier Solution and the Detailed Implementation Plan shall include provisions for major version upgrades of all Software to be promptly upgraded following release of the latest version in accordance with the provisions of Call Off Schedule 2 (Requirements) throughout the Call Off Contract Period unless:

10.4.1 upgrading such Software reduces the level of mitigations for known threats, vulnerabilities or exploitation techniques, provided always that such upgrade is made within twelve (12) Months of release of the latest version; or

10.4.2 an alternative approach is agreed with the Customer in writing.

10.5 The Supplier shall:

10.5.1 implement a mechanism for receiving, analysing and acting upon threat information supplied by NCSC or any other competent public sector organisation;

10.5.2 ensure that NCSC recommended best practice to facilitate the detection of anomalous behaviour that would be indicative of system compromise and report to the Customer such behaviour;

10.5.3 ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the Services technical environment by actively monitoring the threat landscape;

10.5.4 pro-actively scan the Services technical environment for vulnerable Components and address discovered vulnerabilities through the processes described in the ISMS as developed under paragraph 4 of this Call Off Schedule 7;

10.5.5 from the date specified in the Security Management Plan (and before the Operational Service Commencement Date) provide a report to the Customer within five (5) Working Days of the end of each Month detailing both patched and outstanding vulnerabilities in the Services technical environment (to the extent that such environment is within the control of the Supplier) and any 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;

10.5.6 propose interim mitigation measures to vulnerabilities in the Services technical environment known to be exploitable where a security patch is not immediately available;

10.5.7 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 Solution and Services technical environment); and

10.5.8 inform the Customer when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the Services technical environment and provide initial indications of possible mitigations.

10.6 If the Supplier is unlikely to be able to mitigate any vulnerability within the timescales under this paragraph 10 of this Call Off Schedule 7, the Supplier shall immediately notify the Customer.

10.7 A failure to comply with paragraph 10.2 of this Call Off Schedule 7 shall constitute a material Default, and the Supplier shall comply with the Rectification Plan Process.

11. SYSTEM SAFETY

The Parties acknowledge that “System Safety” is about the management of risks related to systems whose anomalous behaviour could affect the physical safety or security of its users or the general public. It is separate from health and safety which deals more with physical risks associated with the use of equipment or the local environment or infrastructure.

ANNEX 1:

National Minimum Cyber Security Standard

The Supplier shall, as a minimum, comply with the Government's National Minimum Cyber Security Standard across all areas of service operation, which as at the Call Off Commencement Date can be found here - https://www.gov.uk/government/publications/the-minimum-cyber-security-standard, as amended and updated from time to time.

This shall be the 'baseline' operating position that will be augmented by the solution specific controls identified within Call Off Schedule 2 (Requirements).

ANNEX 2:

Security Management Plan (Draft)

Supplier Response

We understand that the security of sensitive data is paramount to the delivery of justice. To that end, Konica Minolta and our partners are committed to ensuring we deliver a secure and fit for purpose solution, with the appropriate control mechanisms in place.

What follows is a full scope of content for our Security Management Plan (highlighted in grey), as well as an excerpt of the initial stages. It is not possible to provide our full plan within the 15 page limit, but, should CPS wish to review it in its entirety, it is available upon request. The below is a draft only, and Konica Minolta will work with CPS to ensure that the plan is mutually acceptable to both parties.

The CPS claims an exemption from publishing this information under Section 43(1) of the FOI Act 2000

Annex 3 – Accreditation / Assurance Strategy

The CPS claims an exemption from publishing this information under Section 43(1) of the FOI Act 2000