AUTHORITY: The Secretary of State for the Home Department

Schedule 2.4
Security Management

Gatwick Estate
(Brook House IRC, Tinsley House IRC with Pre-Departure Accommodation)
Immigration Removal Centres and PDA Contract

1. Definitions

In this Schedule, the following definitions shall apply:

"Risk Management Documentation"	has the meaning given in Paragraph 6.3;
"Information Management System"	means the Core Information Management System;
"Accreditation"	the assessment of the Core Information Management System in accordance with Paragraph 6 by the Authority or an independent information risk manager/professional appointed by the Authority, which results in an Accreditation Decision;
"Accreditation Evidence Decision"	is the decision of the Authority, taken in accordance with the process set out in Paragraph 6, 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 Authority, which is prepared by the Supplier and approved by the Authority in accordance with Paragraph 6.4;
"Breach of Security"	the occurrence of: (a) any unauthorised access to or use of the Services, the Authority Premises, the Sites, the Supplier System, the Authority System and/or any information or data (including the Confidential Information and the Authority Data) used by the Authority, the Supplier or any Sub-contractor in connection with this Agreement; (b) the loss (physical or otherwise) and/or unauthorised disclosure of any information or data (including the Confidential Information and the Authority Data), including copies of such information or data, used by the Authority, the Supplier or any Sub-contractor in connection with this Agreement; 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 Schedule 2.1 (Services Description) and the Baseline Security Requirements;
"Certification Requirements"	the requirements set out in Paragraph 7;
"Core Information Management System"	those information assets, ICT systems and/or Sites which will be used by the Supplier and/or its Sub-contractors to Process Authority Data, together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources), which the Authority has determined in accordance with Paragraph 4.2, shall be subject to Accreditation;
"IT Health Check"	has the meaning given Paragraph 8.1.1;
"Personal Data"	has the meaning given in the Data Protection Legislation
"Personal Data Breach"	has the meaning given in the Data Protection Legislation;
"Personal Data Processing Statement"	sets out: (i) the types of Personal Data which the Supplier and/or its Sub-contractors are Processing on behalf of the Authority; (ii) the categories of Data Subjects whose Personal Data the Supplier and/or its Sub-contractors are Processing on behalf of the Authority; the nature and purpose of such Processing; (iii) the locations at which the Supplier and/or its Subcontractors Process Authority Data; and, (iv) the Protective Measures that the Supplier and, where applicable, its Subcontractors have implemented to protect the Authority Data against a Security Breach including a Personal Data Breach, which shall be prepared by the Supplier in accordance with Paragraph 6.4 of Schedule 2.4 (Security Management) and included in the Risk Management Documentation;
"Process Authority Data"	any operation which is performed on Authority Data, whether or not by automated means, including adapting, altering, collecting, combining, copying, destroying, erasing, organising, publishing retrieving, storing, structuring, transmitting or otherwise using Authority Data;

"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 Authority shall be made to the Core Information System and/or the Risk Management Documentation as a consequence of the occurrence of any of the events set out in Paragraph 6.13.1 to 6.13.8 together with the date on which each such change shall be implemented and the date on which each such change was implemented;
"Risk Management Approval Statement"	a notice issued by the Authority which sets out the information risks associated with using the Core Information Management System and confirms that the Authority is satisfied that the identified risks have been adequately and appropriately addressed and that the residual risks are understood and accepted by the Authority;
"Risk Management Reject Notice"	has the meaning given in Paragraph 6.7.2;
"Security Test"	has the meaning given Paragraph 8.1; and
"Statement of Information Risk Appetite"	has the meaning given in Paragraph 5.1;.
"Vulnerability Correction Plan"	has the meaning given in Paragraph 8.3.3(a);

2. Introduction

2.1 This Schedule sets out:

2.1.1 the principles which the Supplier shall comply with when performing its obligations under this Agreement in order to ensure the security of the Authority Data, the IT Environment, the Supplier Solution and the Information Management System;

2.1.2 the process which shall apply to the Accreditation of the Core Information Management System in Paragraph 6;

2.1.3 the Certification Requirements applicable to the Wider Information Management System in Paragraph 7;

2.1.4 the Security Tests which the Supplier shall conduct during the Term in Paragraph 8;

2.1.5 the Security Tests which the Authority may conduct during the Term in Paragraph 8.6;

2.1.6 the requirements to patch vulnerabilities in the Core Information Management System in Paragraph 9;

2.1.7 the obligations on the Supplier to prevent the introduction of Malicious Software into the Information Management System and to scan for, contain the spread of, and minimise the impact of Malicious Software which is introduced into the Information Management System in Paragraph 10; and

2.1.8 each Party's obligations in the event of an actual or attempted Breach of Security in Paragraph 11.

3. Principles of Security

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

3.1.1 the IT Environment;

3.1.2 the Supplier Solution; and

3.1.3 the Information Management System.

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

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

3.2.2 the security of the Supplier Solution; and

3.2.3 the security of the Information Management System.

3.3 The Governance Group shall, in addition to its responsibilities set out in Schedule 8.1 (Governance), monitor and may also provide recommendations to the Supplier on the Accreditation of the Core Information Management System.

3.4 Each Party shall provide access to members of its information assurance personnel to facilitate the Supplier's design, implementation, operation, management and continual improvement of the Risk Management Documentation and the security of the Supplier Solution and Information Management System and otherwise at reasonable times on reasonable notice.

4. Information Management System

4.1 The Information Management System comprises the Core Information Management System.

4.2 The Supplier shall provide the Authority with such documentation and information that the Authority may reasonably require regarding any information assets, ICT systems and/or Sites which will be used by the Supplier or any Sub-contractor to Process Authority Data together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources).

4.3 Any proposed change to the component parts of and/or boundary of the Core Information Management System shall be notified and processed in accordance with the Change Control Procedure.

5. Statement of Information Risk Appetite and Baseline Security Requirements

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

5.2 The Authority's Baseline Security Requirements in respect of the Core Information Management System are set out in Annex 1.

5.3 The Statement of Information Risk Appetite and the Baseline Security Requirements shall inform the Accreditation of the Core Information Management System.

5.4 The Authority's Statement of Information Risk Appetite is set out in the following table;

Area of Risk	**Type of Risk**	**Approximate Current Risk Arising**	**Risk Appetite**	Risk Tolerance
Systems	Compliance with HO Security principles and rules (incl. GDPR)	Medium	Very Low	Minimal

6. Accreditation of the Core Information Management System

6.1 The Core Information Management System shall be subject to Accreditation in accordance with this Paragraph 6.

6.2 The Accreditation shall be performed by the Supplier or by representatives appointed by the Supplier and evidence of the Accreditation shall be submitted to the Authority.

6.3 Prior to the Operational Services Commencement Date, the Supplier shall prepare and submit to the Authority the risk management documentation for the Core Information Management System, which shall comply with, and be subject to

approval by the Authority in accordance with, this Paragraph 6 (the "**Risk Management Documentation**").

6.4 The Risk Management Documentation shall be structured in accordance with the template as set out in Annex 3 and include:

6.4.1 the Accreditation Plan, which shall include:

(a) the dates on which each subsequent iteration of the Risk Management Documentation will be delivered to the Authority for review and staged approval; and

(b) the date by which the Supplier is required to have received a Risk Management Approval Statement from the Authority together with details of each of the tasks which must be completed by the Supplier, Milestones which must be Achieved and the Authority Responsibilities which must be completed in order for the Supplier to receive a Risk Management Approval Statement pursuant to Paragraph 6.7.1

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

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

6.4.4 unless such requirement is waived by the Authority, proposed controls that will be implemented in respect of all aspects of the Services and all processes associated with the delivery of the Services, including the Authority Premises, the Sites, the Supplier System, the Authority System (to the extent that it is under the control of the Supplier) and any IT, Information and data (including the Authority Confidential Information and the Authority Data) to the extent used by the Authority or the Supplier in connection with this Agreement or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Services;

6.4.5 the Required Changes Register;

6.4.6 evidence that the Supplier and each applicable Sub-contractor is compliant with the Certification Requirements; and

6.4.7 a Personal Data Processing Statement.

6.5 If the Risk Management Documentation submitted to the Authority pursuant to Paragraph 6.3 (or Paragraph 6.10, as applicable) is approved by the Authority, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Risk Management

Documentation is not approved by the Authority, the Supplier shall amend it within 10 Working Days of a notice of non-approval from the Authority and re-submit it to the Authority for approval. 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 15 Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Authority. If the Authority does not approve the Risk Management Documentation following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Authority pursuant to this Paragraph may be unreasonably withheld or delayed. However, any failure to approve the Risk Management Documentation on the grounds that it does not comply with the requirements set out in Paragraph 6.4 shall be deemed to be reasonable.

6.6 The Supplier shall provide any information and/or documentation that the Authority or its representative may reasonably require, to enable the Authority to establish that the Accredited Core Information System is compliant with the Risk Management Documentation.

6.7 The Authority shall, by the relevant date set out in the Accreditation Plan, review the review the evidence of accreditation provided by the Supplier and issue to the Supplier either:

6.7.1 a Risk Management Approval Statement which will then form part of the Risk Management Documentation, confirming that the Authority is satisfied that the identified risks to the Core Information Management System have been adequately and appropriately addressed and that the residual risks are understood and accepted by the Authority; or

6.7.2 a rejection notice stating that the Authority considers that the accreditation evidence provided by the Supplier identifies residual risks to the Core Information Management System which have not been reduced to a level acceptable by the Authority and the reasons why (**"Risk Management Rejection Notice"**).

6.8 If the Authority issues a Risk Management Rejection Notice, the Supplier shall, within 20 Working Days of the date of the Risk Management Rejection Notice:

6.8.1 address all of the issues raised by the Authority in such notice; and

6.8.2 notify the Authority that the Core Information Management System is ready for an Accreditation Evidence Decision.

6.9 If the Authority determines that the Supplier's actions taken pursuant to the Risk Management Rejection Notice have not reduced the residual risks to the Core Information Management System to an acceptable level and issues a further Risk Management Rejection Notice, the failure to receive a Risk Management Approval Statement shall constitute a material Default and the Authority may by terminate this Agreement with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 33.1(b).

6.10 The process set out in Paragraph 6.7 and Paragraph 6.8 shall be repeated until such time as the Authority issues a Risk Management Approval Statement to the Supplier or terminates this Agreement.

6.11 The Supplier acknowledges that it shall not be permitted to use the Core Information Management System to Process Authority Data prior to receiving a Risk Management Approval Statement.

6.12 The Supplier shall keep the Core Information Management System and Risk Management Documentation under review and shall update the Risk Management Documentation annually in accordance with this Paragraph and the Authority shall review the Accreditation Decision annually and following the occurrence of any of the events set out in Paragraph 6.13.

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

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

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

6.13.3 a change in the threat profile;

6.13.4 a Sub-contractor failure to comply with the Core Information Management System code of connection;

6.13.5 a significant change to any risk component;

6.13.6 a significant change in the quantity of Personal Data held within the Core Information Management System;

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

6.13.8 an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns,

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

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

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

6.14.2 where such Default is capable of remedy, the Supplier shall remedy such Default within the timescales set by the Authority and, should the Supplier fail to remedy the Default within such timescales, the Authority may terminate this Agreement with

immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 33.1(b).

6.15 The Supplier shall review each Change Request against the Risk Management Documentation 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 Risk Management Documentation, the Supplier shall set out any proposed amendments to the documentation in the Impact Assessment associated with such Change Request for consideration and approval by the Authority.

6.16 The Supplier shall be solely responsible for the costs associated with developing and updating the Risk Management Documentation and carrying out any remedial action required by the Authority as part of the Accreditation process.

7. Certification Requirements

7.1 The Supplier shall ensure, at all times during the Term, that the Supplier and any Sub-contractor with access to Authority Data or who will Process Authority Data are certified as compliant with:

7.1.1 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

7.1.2 Cyber Essentials PLUS,

and shall provide the Authority with a copy of each such certificate of compliance before the Supplier or the relevant Sub-contractor (as applicable) shall be permitted to use the Core Information Management System to receive, store or Process any Authority Data. Any exceptions to the flow-down of the certification requirements to third party suppliers and sub-contractors must be agreed with the Authority.

7.2 The Supplier shall ensure, at all times during the Term, that the Supplier and each Sub-contractor who is responsible for the secure destruction of Authority Data:

7.2.1 securely destroys Authority Data only on Sites which are included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; and

7.2.2 are certified as compliant with the NCSC Assured Service (CAS) Service Requirement Sanitisation Standard or an alternative standard as agreed by the Authority.

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

7.3 The Supplier shall notify the Authority as soon as reasonably practicable and, in any event within 2 Working Days, if the Supplier or any Sub-contractor ceases to be compliant with the Certification Requirements and, on request from the Authority, shall or shall procure that the relevant Sub-contractor shall:

7.3.1 immediately ceases using the Authority Data; and

7.3.2 procure that the relevant Sub-contractor promptly returns, destroys and/or erases the Authority Data in accordance with Baseline Security Requirements.

8. Security Testing

8.1 The Supplier shall, at its own cost and expense:

8.1.1 procure a CHECK IT Health Check of the Core Information Management System (an "**IT Health Check**") by a NCSC approved member of the CHECK Scheme:

(a) prior to it submitting the Risk Management Documentation to the Authority for an Accreditation Evidence Decision;

(b) if directed to do so by the Authority in accordance with Paragraph 8.2; and

(c) once every 12 months during the Term.

8.1.2 conduct vulnerability scanning and assessments of the Core Information Management System monthly;

8.1.3 conduct an assessment as soon as reasonably practicable following receipt by the Supplier or any of its Sub-contractors 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

8.1.4 conduct such other tests as are required by:

(a) any Vulnerability Correction Plans;

(b) the ISO27001 certification requirements;

(c) the Risk Management Documentation; and

(d) the Authority following a Breach of Security or a significant change to the components or architecture of the Core Information Management System,

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

8.2 The Supplier shall provide the Authority with the results of such Security Tests (in a form approved by the Authority in advance) as soon as practicable after completion of each Security Test.

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

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

8.3.2 promptly, following receipt of each IT Health Check report, provide the Authority with a copy of the IT Health Check report;

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

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

(i) how the vulnerability will be remedied;

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

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

(b) comply with the Vulnerability Correction Plan; and

(c) 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.

8.4 The Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Authority. Subject to the Supplier complying with this Paragraph 8.4, if a Security Test causes a Performance Failure in a particular Measurement Period, the Supplier shall be granted relief in respect of such Performance Failure for that Measurement Period.

8.5 The Authority shall be entitled to send a representative to witness the conduct of the Security Tests. Without prejudice to the Supplier's obligations under Paragraph 8.3, the Supplier shall provide the Authority with the results of such Security Tests (in a form approved by the Authority in advance) as soon as practicable after completion of each Security Test.

8.6 The Authority and/or its authorised representatives shall be entitled, at any time and without giving notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the Service, the Information System and/or the Supplier's compliance with the Risk Management Documentation ("**Authority Security Tests**"). The Authority shall take reasonable steps to notify the Supplier prior to carrying out such Authority Security Test to the extent that it is reasonably practicable for it to do so taking into account the nature of the Authority Security Test.

8.7 The Authority shall notify the Supplier of the results of such Authority Security Tests after completion of each Authority Security Test.

8.8 The Authority Security Tests shall be designed and implemented so as to minimise their impact on the delivery of the Services. If an Authority Security Test causes a

Performance Failure in a particular Measurement Period, the Supplier shall be granted relief in respect of such Performance Failure for that Measurement Period.

8.9 Without prejudice to the provisions of Paragraph 8.3.3, where any Security Test carried out pursuant to this Paragraph 8 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 Authority of any changes to the Core Information Management System and/or the Risk Management Documentation (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Authority's prior written approval, the Supplier shall implement such changes to the Core Information Management System and/or the Risk Management Documentation and repeat the relevant Security Tests in accordance with the timetable agreed with the Authority or, otherwise, as soon as reasonably possible.

8.10 If the Authority unreasonably withholds its approval to the implementation of any changes proposed by the Supplier to the Risk Management Documentation in accordance with Paragraph 8.8 above, the Supplier shall not be deemed to be in breach of this Agreement to the extent it can be shown that such breach:

8.10.1 has arisen as a direct result of the Authority unreasonably withholding its approval to the implementation of such proposed changes; and

8.10.2 would have been avoided had the Authority given its approval to the implementation of such proposed changes.

8.11 For the avoidance of doubt, where a change to the Core Information Management System and/or the Risk Management Documentation is required to remedy non-compliance with the Risk Management Documentation, the Baseline Security Requirements and/or any obligation in this Agreement, the Supplier shall effect such change at its own cost and expense.

8.12 If any repeat Security Test carried out pursuant to Paragraph 8.9 reveals an actual or potential Breach of Security or weakness exploiting the same root cause failure, such circumstance shall constitute a material Default and the Authority may by terminate this Agreement with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause [33.1(b)].

8.13 The Supplier shall, by of each contract year, during the Term, provide to the Authority a letter from its chief executive officer (or equivalent officer) confirming that having made due and careful enquiry:

8.13.1 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 Agreement; and

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

9. Vulnerabilities and Corrective Action

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

9.2 The severity of vulnerabilities for Supplier COTS Software and Third Party COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the agreed method in the Risk Management Documentation and using the appropriate vulnerability scoring systems including:

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

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

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

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

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

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

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

9.4.1 the Supplier can demonstrate that a vulnerability in the Core Information Management System is not exploitable within the context of the Services (e.g. because it resides in a Software component which is not involved in running in the Services) provided such vulnerabilities shall be remedied by the Supplier within the timescales set out in Paragraph 9.3 if the vulnerability becomes exploitable within the context of the Services;

9.4.2 the application of a '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 Authority; or

9.4.3 the Authority agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the Risk Management Documentation.

9.5 The Risk Management Documentation shall include provisions for major version upgrades of all Supplier COTS Software and Third Party COTS Software to be kept up to date such that all Supplier COTS Software and Third Party COTS Software are always in mainstream support throughout the Term unless otherwise agreed by the Authority in writing.

9.6 The Supplier shall:

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

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

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

9.6.4 ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the Core Information Management System by actively monitoring the threat landscape during the Term;

9.6.5 pro-actively scan the Core Information Management System for vulnerable components and address discovered vulnerabilities through the processes described in the Risk Management Documentation;

9.6.6 from the date specified in the Accreditation Plan and within 5 Working Days of the end of each subsequent month during the Term, provide the Authority with a written report which details both patched and outstanding vulnerabilities in the Core Information Management System, the elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report and any failure to comply with the timescales set out in Paragraph 9.3 for applying patches to vulnerabilities in the Core Information Management System;

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

9.6.8 remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the Core Information Management System); and

9.6.9 inform the Authority when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the Core Information Management System and provide initial indications of possible mitigations.

9.7 If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under Paragraph 10, the Supplier shall immediately notify the Authority.

9.8 If the Supplier fails to patch vulnerabilities in the Core Information Management System in accordance with Paragraph 9.3, such failure shall constitute a material Default and the Authority may by terminate this Agreement with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 33.1(b).

10. Malicious Software

10.1 The Supplier shall install and maintain anti-Malicious Software or procure that latest versions of anti-virus definitions and anti-Malicious Software is installed and

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

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

10.3 any cost arising out of the actions of the Parties taken in compliance with the provisions of Paragraph 10.2 shall be borne by the Parties as follows:

10.3.1 by the Supplier where the Malicious Software originates from the Supplier Software, the Third Party Software supplied by the Supplier (except where the Authority has waived the obligation set out in Clause 20.13) or the Authority Data (whilst the Authority 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 Authority when provided to the Supplier; and

10.3.2 otherwise by the Authority.

11. Breach of Security

11.1 If either Party becomes aware of a Breach of Security or an attempted Breach of Security it shall notify the other in accordance with the security incident management process as set out in the Risk Management Documentation.

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

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

(a) minimise the extent of actual or potential harm caused by such Breach of Security;

(b) remedy such Breach of Security to the extent possible and protect the integrity of the Information System against any such potential or attempted Breach of Security;

(c) apply a tested mitigation against any such Breach of Security or potential or attempted Breach of Security and, provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier's ability to deliver the Services so as to meet any Performance Indicator, the Supplier shall be granted relief against the failure to meet such affected Performance Indicator

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

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

11.2.2 as soon as reasonably practicable and, in any event, within 2 Working Days, following the Breach of Security or attempted Breach of Security, provide to the Authority full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Authority.

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

11.4 If the Supplier fails to comply with its obligations set out in this Paragraph 11, such failure shall constitute a material Default, which if not remedied to the satisfaction of the Authority, shall permit the Authority to terminate this Agreement with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 33.1(b).

12. Data Processing, Storage, Management and Destruction

12.1 In addition to the obligations on the Supplier set out Clause 23 (Protection of Personal Data) in respect of Processing Personal Data and compliance with the DPA, the Supplier shall:

12.1.1 Process Authority Data only at the Sites and such Sites must not located outside of the European Union except where the Authority has given its consent to a transfer of the Authority Data to outside of the European Union in accordance with Clause 23;

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

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

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

12.1.5 securely destroy all media that has held Authority Data at the end of life of that media in accordance with any specific requirements in this Agreement and, in the absence of any such requirements, as directed by the Authority.

Annex 1: Baseline Security Requirements

1. Security Classification of Information

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

1.1 OFFICIAL or OFFICIAL-SENSITIVE, the Supplier shall implement such additional measures as agreed with the Authority from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards; and/or

1.2 SECRET or TOP SECRET, the Supplier shall only do so where it has notified the Authority prior to receipt of such Authority Data and the Supplier shall implement additional measures as agreed with the Authority from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards.

2. End User Devices

2.1 The Supplier shall ensure that any Authority 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 Authority except where the Authority has given its prior written consent to an alternative arrangement.

2.2 The Supplier shall ensure that any device which is used to Process Authority 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. Networking

The Supplier shall ensure that any Authority 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.

4. Personnel Security

4.1 All Supplier Personnel shall be subject to a pre-employment check before they may participate in the provision and or management of the Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; verification of the individual's criminal record.

4.2 The Authority and the Supplier shall review the roles and responsibilities of the Supplier Personnel who will be involved in the management and/or provision of the Services in order to enable the Authority to determine which roles require additional vetting and a specific national security vetting clearance (e.g. a Counter Terrorist Check; a Security Check). Roles which are likely to require additional vetting and a specific national security vetting clearance include system administrators whose

role would provide those individuals with privileged access to IT systems which Process Authority Data or data which is classified as OFFICIAL-SENSITIVE.

4.3 The Supplier shall not permit Supplier Personnel who fail the security checks required by Paragraphs 4.1 and 4.2 to be involved in the management and/or provision of the Services except where the Authority has expressly agreed in writing to the involvement of the named individual in the management and/or provision of the Services.

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

4.5 The Supplier shall ensure that Supplier Personnel who no longer require access to the Authority Data (e.g. they cease to be employed by the Supplier or any of its Sub-contractors), have their rights to access the Authority Data revoked within 1 Working Day.

5. Identity, Authentication and Access Control

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

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

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

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

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

6. Audit and Protective Monitoring

6.1 The Supplier shall collect audit records which relate to security events in Core Information Management System or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include regular reports and alerts setting out details of access by users of the Core Information Management System, to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of Authority Data.

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

6.3 The retention periods for audit records and event logs must be agreed with the Authority and documented in the Risk Management Documentation.

7. Secure Architecture

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

7.1.1 the NCSC "Security Design Principles for Digital Services", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/security-design-principles-digital-services-main;

7.1.2 the NCSC "Bulk Data Principles", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main; and

7.1.3 the NSCS "Cloud Security Principles", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles and which are summarised below:

(a) "Cloud Security Principle 1: data in transit protection" which, amongst other matters, requires that user data transiting networks should be adequately protected against tampering and eavesdropping;

(b) "Cloud Security Principle 2: asset protection and resilience" which, amongst other matters, requires that user data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure;

(c) "Cloud Security Principle 3: separation between users" which, amongst other matters, requires that a malicious or compromised user of the service should not be able to affect the service or data of another;

(d) "Cloud Security Principle 4: governance framework" which, amongst other matters, requires that the Supplier should have a security governance framework which coordinates and directs its management of the Services and information within it;

(e) "Cloud Security Principle 5: operational security" which, amongst other matters, requires that the Services need to be operated and managed securely in order to impede, detect or prevent a Breach of Security;

(f) "Cloud Security Principle 6: personnel security" which, amongst other matters, requires that where Supplier Personnel have access to Authority Data and/or the Authority System that those personnel be subject to appropriate security screening and regular security training;

(g) "Cloud Security Principle 7: secure development" which, amongst other matters, requires that the Services be designed and developed to identify and mitigate threats to their security;

(h) "Cloud Security Principle 8: supply chain security" which, amongst other matters, requires the Supplier to ensure that appropriate security controls are in place with its Sub-contractors and other suppliers;

(i) "Cloud Security Principle 9: secure user management" which, amongst other matters, requires the Supplier to make the tools available for the Authority to securely manage the Authority's use of the Service;

(j) "Cloud Security Principle 10: identity and authentication" which, amongst other matters, requires the Supplier to implement appropriate controls in order to ensure that access to Service interfaces is constrained to authenticated and authorised individuals;

(k) "Cloud Security Principle 11: external interface protection" which, amongst other matters, requires that all external or less trusted interfaces with the Services should be identified and appropriately defended;

(l) "Cloud Security Principle 12: secure service administration" which, amongst other matters, requires that any ICT system which is used for administration of a cloud service will have highly privileged access to that service;

(m) "Cloud Security Principle 13: audit information for users" which, amongst other matters, requires the Supplier to be able to provide the Authority with the audit records it needs to monitor access to the Service and the Authority Data held by the Supplier and/or its Sub-contractors;

(n) "Cloud Security Principle 14: secure use of the service" which, amongst other matters, requires the Supplier to educate Supplier Personnel on the safe and secure use of the Information Management System.

Annex 2 – Attached (Page 1 of 2)

CORE INFORMATION MANAGEMENT SYSTEM DIAGRAM

Annex 2 – Attached (Page 2 of 2)

CORE INFORMATION MANAGEMENT SYSTEM DIAGRAM

Annex 3

Risk Management Documentation Template

Author:

Owner:

Date:

Version:

1 EXECUTIVE SUMMARY

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

List of Contents

Change History

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

References, Links and Dependencies

This document is dependent on the supporting information and assurance provided by the following documents.

ID	Document Title	Reference	Date
1.			
2.			
3.			

2 SYSTEM DESCRIPTION

2.1 Background

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

2.2 Organisational Ownership/Structure

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

2.3 Information assets and flows

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

2.4 System Architecture

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

2.5 Users

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

2.6 Locations

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

2.7 Test and Development Systems

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

2.8 Key roles and responsibilities

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

3 RISK ASSESSMENT

3.1 Accreditation/Assurance Scope

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

3.2 Risk appetite

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

3.3 Business impact assessment

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

3.4 Risk assessment

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

Risk ID	Inherent risk	Inherent risk level	Vulnerability	Controls	Residual risk level
R1	Internet attackers could hack the system.	Medium	The service systems are exposed to the internet via the web portal.	C1: Internet-facing firewalls C2: Internet-facing IP whitelist C3: System hardening C4: Protective monitoring C5: Application access control C16: Anti-virus for incoming files C54: Files deleted when processed C59: Removal of departmental identifier	Very low

Risk ID	Inherent risk	Inherent risk level	Vulnerability	Controls	Residual risk level
R2	Remote attackers could intercept or disrupt information crossing the internet.	Medium	File sharing with organisations across the internet.	C9: TLS communications C10: PGP file-sharing	Very low
R3	Internal users could maliciously or accidentally alter bank details.	Medium-High	Users bank details can be altered as part of the normal business function.	C12. System administrators hold SC clearance. C13. All changes to user information are logged and audited. C14. Letters are automatically sent to users home addresses when bank details are altered. C15. Staff awareness training	Low

3.5 **Controls**

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

ID	Control title	Control description	Further information and assurance status
C1	Internet-facing firewalls	Internet-facing firewalls are in place between the internet and the system', which restrict access from the internet to the required ports only.	Assured via ITHC firewall rule check
C2	Internet-facing IP whitelist	An IP whitelist is in place for all access from the internet.	Assured via ITHC
C15	Staff awareness training	All staff must undertake annual security awareness training and this process is audited and monitored by line managers.	Assured as part of ISO27001 certification

3.6 **Residual risks and actions**

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

4 IN-SERVICE CONTROLS

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

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

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

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

d) *configuration and change management;*

e) *incident management;*

f) *vulnerability management;*

g) *user access management; and*

h) data sanitisation and disposal.>

5 SECURITY OPERATING PROCEDURES (SYOPS)

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

6 MAJOR HARDWARE AND SOFTWARE AND END OF SUPPORT DATES

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

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

7 INCIDENT MANAGEMENT PROCESS

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

8 SECURITY REQUIREMENTS FOR USER ORGANISATIONS

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

9 REQUIRED CHANGES REGISTER

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

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

10 PERSONAL DATA PROCESSING STATEMENT

<This should include: (i) the types of Personal Data which the Supplier and/or its Sub-contractors are Processing on behalf of the Authority; (ii) the categories of Data Subjects whose Personal Data the Supplier and/or its Sub-contractors are Processing on behalf of the Authority; the nature and purpose of such

Processing; (iii) the locations at which the Supplier and/or its Subcontractors Process Authority Data; and, (iv) the Protective Measures that the Supplier and, where applicable, its Subcontractors have implemented to protect the Authority Data against a Security Breach including a Personal Data Breach.>

11 ANNEX A. ISO27001 AND/OR CYBER ESSENTIAL PLUS CERTIFICATES

<Any certifications relied upon should have their certificates included>

12 Annex B. Cloud Security Principles assessment

<A spreadsheet may be attached>

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

<A spreadsheet may be attached>

14 Annex E. Latest ITHC report and Vulnerability Correction Plan