TCN SCHEDULE 2.4

SECURITY MANAGEMENT

Security Management

1. Definitions

In this Schedule, the following definitions shall apply:

"**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 Systemand/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), includingcopies 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 (where relevant) 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;
"Authority Data"	shall have the meaning given to it in Schedule 1 (Definitions) and for the purposes of this Schedule only shall include (to the extent the same is not already included in the Schedule 1 definition) the following: (a) operational data (including Personal Data), whether in the live production system of the Core Information Management System, or elsewhere, including logging data; (b) Personal Data that is not sufficiently pseudonymised or otherwise de-

	identified to the Authority's satisfaction; (c) Configuration data for the Core Information Management System, whether within that system (which includes the means of system delivery, including its development) or elsewhere; and (d) Information, documentation and code relating to the design or operation of the Core Information Management System.
"Confidential Information"	shall have the meaning given to it in Schedule 1 (Definitions) and for the purposes of this Schedule only shall include (to the extent the same is not already included in the Schedule 1 definition) the following: data not defined as "Authority Data" that relates to the design, delivery, support, operation of the Services or commercial agreements and information pertaining to the Services that are considered OFFICAL or OFFICIAL SENSITIVE and are not in the public domain;
"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 and/or deliver and support the Services, 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 Security Assurance;
"Information Management System"	means the Core Information Management System and the Wider Information Management System;
"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 Sub-contractors 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 Breach of Security including a Personal Data Breach, which shall be prepared by the Supplier in accordance with Paragraph 6.4 and included in the Security Assurance 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;
“Real Data”	includes but is not limited to: (a) live production data (the databases within the production environment, including Personal Data);. (b) replicas or partial replicas of the data specified in (a), in any environment; (c) data being migrated to the Core Information Management System; (d) any extract of (a) – (c) above (for example, individual records, tables or partial forms thereof, in any environment); (e) output data and logs that include Real Data (for example, error logs with Real Data within them); and (f) management information reports;
"Required Changes Register"	is a register which forms part of the Security Assurance Documentation which records each of the changes that the Supplier has agreed with the Authority shall

	be made to the Core Information Management System and/or the Security Assurance Documentation as aconsequence of the occurrence of any of the events set out in Paragraph 6.14.1 to 6.14.8 together with the date on which each such change shall be implemented and the date on which each such change was implemented;
"Security Assurance Approval Statement"	a notice (which the Authority, in the usual course of business, terms an "*Authority to Operate*") 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;
"Security Assurance Rejection Notice"	has the meaning given in Paragraph 6.7.2;
"Security Assurance"	the assessment of the Core Information Management System in accordance with Paragraph 6 by the Authority (or an independent information risk manager/professional appointed on behalf of the Authority), the consequence of which is a Security Assurance Decision;
"Security Assurance Decision"	is the decision of the Authority, taken in accordance with the process set out in Paragraph 6, to issue the Supplier with either a Security Assurance Approval Statement or a Security Assurance Rejection Notice in respect of the Core Information Management System;
"Security Assurance Documentation"	has the meaning given in Paragraph 6.3;
"Security Assurance Plan"	the Supplier's plan to attain Security Assurance Approval Statements from the Authority at key events, which is prepared by the Supplier and approved by the Authority in accordance with Paragraph 6.4;
"Security Test"	has the meaning given Paragraph 8.1;

"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); and
"Wider 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 and/or deliver the Services which have not been determined by the Authority to form part of the Core Information Management System together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources.

2. 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 Security Assurance 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 monitor and 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.

2.2 The Supplier shall also comply with the provisions of the Baseline Security Requirements set out in Annex 1, which is a non-exhaustive statement of lower-level security requirements that the Authority requires the Supplier to

observe in its approach to, implementation of and assurance of the security of the Services and the Supplier System, the means of development and delivery of the Services and the Supplier System, and the operation and support of the Services and the Supplier System where conducted by the Supplier.

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 the provision of the Services and, consequently on the security of:

3.1.1 the IT Environment;

3.1.2 the Supplier Solution including any hosting, development and support environments;

3.1.3 Service delivery environments, such as test centres; and

3.1.4 the Information Management System.

3.2 Notwithstanding the involvement of the Authority in the Security Assurance 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 Audit Assurance Board shall, in addition to its responsibilities set out in Schedule 8.1 (Governance), monitor and may also provide recommendations to the Supplier on the Security Assurance 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 Security Assurance 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 and the Wider Information Management System.

4.2 The Authority shall be responsible for determining the boundary between the Core Information Management System and the Wider Information Management System. In order to enable the Authority to make such determination, the Supplier shall provide the Authority (within 15 days following the Effective Date) 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). The Authority shall notify the Supplier, as soon as reasonably practical following the receipt of such documentation and information, of its decision regarding the component parts of the Core Information Management System and its boundary with the Wider Information Management System.

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 Security Assurance of the Core Information Management System.

6. Security Assurance of the Core Information Management System

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

6.2 The Security Assurance shall be performed by the Authority or by representatives appointed by the Authority.

6.3 The Supplier shall prepare (or update as necessary) and submit to the Authority the security assurance 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 "**Security Assurance Documentation**"), at the following points in time:

6.3.1 prior to connecting any part of the Core Information Management System that is intended to contain Real Data to external systems, including the Internet;

6.3.2 prior to loading any part of the Core Information Management System with Real Data;

6.3.3 prior to the first Operational Services Commencement Date.

6.4 The Security Assurance Documentation shall be structured in accordance with the template as set out in Annex 3 and include (but not limited to):

6.4.1 the Security Assurance Plan, which shall include but not be limited to:

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

(b) the dates by which the Supplier is required to have received Security Assurance Approval Statements 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 Security Assurance 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 the extent that it is under the control of the Supplier) and any IT, Information and data (including the Authority's 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 Security Assurance 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 Security Assurance 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 Security Assurance 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 Security Assurance 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 To facilitate Security Assurance of the Core Information Management System, the Supplier shall provide the Authority and its authorised representatives with:

6.6.1 access to the Sites, ICT information assets and ICT systems or any other assets used in delivery of the Services within the Core Information Management System on request or in accordance with the Security Assurance Plan; and

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

6.7 The Authority shall, by the relevant date set out in the Security Assurance Plan, review the identified risks to the Core Information Management System and issue to the Supplier either:

6.7.1 a Security Assurance Approval Statement which will then form part of the Security Assurance 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 residual risks to the Core Information Management System have not been reduced to a level acceptable by the Authority and the reasons why ("**Security Assurance Rejection Notice**").

6.8 If the Authority issues a Security Assurance Rejection Notice, the Supplier shall, within 20 Working Days of the date of the Security Assurance 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 a Security Assurance Decision.

6.9 If the Authority determines that the Supplier's actions taken pursuant to the Security Assurance Rejection Notice have not reduced the residual risks to the Core Information Management System to an acceptable level and issues a further Security Assurance Rejection Notice, the failure to receive a Security Assurance Approval Statement shall constitute a material Default and the Authority may terminate this Agreement with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 33.1.2.

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 Security Assurance 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 Security Assurance Approval Statement.

6.12 The Supplier shall keep the Core Information Management System and Security Assurance Documentation under review and shall update the Security Assurance Documentation not less than annually in accordance with this Paragraph and more frequently (as required by the Authority) following the occurrence of any of the events set out in Paragraph 6.14.

6.13 The Authority shall review the Security Assurance Decision not less than quarterly and following the occurrence of any of the events set out inParagraph 6.14.

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

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

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

6.14.3 a change in the threat profile (and the Supplier shall continually assess the threat profile in order to comply with this paragraph);

6.14.4 a Sub-contractor failure to comply with the Core Information Management System security requirements;

6.14.5 a significant change to any risk component;

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

6.14.7 a proposal to change any of the Sites (including any third-party or Sub-contractor sites from which any computing services are provided) from which any part of the Services are provided; and/or

6.14.8 an ISO27001 (or equivalent authorised in writing by the Authority) 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.

6.15 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:

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

6.15.2 where such Default is capable of remedy, the Supplier shall remedy such Default within the timescales reasonably required 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 33.1.2.

6.16 The Supplier shall review each Change Request against the Security Assurance 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 Security Assurance 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.

6.17 The Supplier shall be solely responsible for the costs associated with developing and updating the Security Assurance Documentation and carrying out any remedial action required by the Authority as part of the Security Assurance 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, or who will develop code, or supply services such as hosting that support the Services are certified as compliant with relevant standards including (but not limited to):

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.

7.3 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.

7.4 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:

7.4.1 immediately ceases using the Authority Data; and

7.4.2 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 an independent 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 Security Assurance Documentation to the Authority for an Security Assurance Decision;

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

(c) as a minimum 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 Security Assurance 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 of report 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 of report 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 Management System and/or the Supplier's compliance with the Security Assurance 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 Security Assurance 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 Security Assurance 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 Security Assurance Documentation in accordance with Paragraph 8.9 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 Security Assurance Documentation is required to remedy non-compliance with the Security Assurance 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 terminate this Agreement with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 33.1.2.

8.13 The Supplier shall, by no later than 12 months following the Effective Date (and thereafter every 12 months 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

This section is redacted due to sensitivity around security

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 software and definition updates (which can be automatic where agreed in writing by the Authority) 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 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

Redacted

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 Data Protection Legislation, the Supplier shall:

12.1.1 Process Authority Data only at the Sites and such Sites must not be 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

1.1 All components, services, personnel and locations involved in delivery of the Future Theory Test service (including the Digital Integrator, the Test Centre Network and the Test Engine and Test Content Management System) need to align with a consistent set of security requirements, principles and practices in order to avoid introducing undesirable vulnerabilities and weaknesses into the service. To that end this Annex contains both a high level description of overarching key baseline security measures, and then in paragraph 8 a more detailed set of controls, measures and procedures that the Future Theory Test service as a whole (including the Digital Integrator, the Test Centre Network and the Test Engine and Test Content Management System) is expected to meet and which need to be supported by the individual contracted services across the project lifecycle. This includes:

(a) the design of the service, including technical components, procedures and locations;

(b) the implementation of components including code development, testing, QA;

(c) the transition of the service into live operation;

(d) the operation of the service including eg incident management, business continuity

(e) support arrangements including service management, changes;

(f) decommissioning of the service, sites, and deletion of data.

1.2 These requirements reflect both the existing Authority security policies, overall corporate Authority Risk Appetite, HMG guidance and principles and Good Industry Practice.

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

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

1.3.2 Redacted

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 aproduct 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 (to an appropriate standard as agreed in writing with the Authority) 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 such as a specific National Security vetting clearance (e.g. a Counter Terrorist Check; a Security Check). Roles which arelikely to require additional vetting include system administrators, security team members and system architects 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 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.

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

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

6. Audit and Protective Monitoring

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

8. Detailed Security requirement set

8.1 This detailed statement of security requirements reflects the expected approach to, implementation of and assurance of security by the suppliers of Theory Test systems, solutions and services.

8.2 The Supplier is reminded of the following legislation that is relevant to the security requirements:

8.2.1 The Supplier shall identify and comply with all relevant legislative statutory, regulatory and contractual requirements.

8.2.2 The Supplier shall identify future relevant legislative statutory, regulatory and contractual requirements and plan to prepare to meet their requirements.

8.2.3 At present the list of applicable security-related legislation includes:

(a) Data Protection Legislation;

(b) Freedom of Information Act 2000;

(c) Public Records Act 1958;

(d) Official Secrets Act 1989;

(e) Environmental Information Regulations 2004;

(f) Pre-Release Access to Official Statistics Order 2008;

8.2.4 The list of applicable legislation shall be interpreted as these and their successors.

8.2.5 The Supplier shall use cryptographic controls in compliance with all relevant agreements, legislation and regulations.

8.3 The following requirements related to data apply.

8.3.1 The Supplier must implement measures as agreed with the Authority from time to time in order to ensure that information is safeguarded in accordance with the applicable standards for OFFICIAL-SENSITIVE data.

8.3.2 The Supplier must 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 data to outside the European Union.

8.3.3 The Supplier must meet the standards of the Authority's Personal Information Charter regarding the handling of Personal Data: https://www.gov.uk/government/organisations/driver-and-vehicle-standards-agency/about/personal-information-charter.

8.3.4 The Supplier must only use personally identifiable data or other strategic Real Data in a system which has been:

(a) subject to a relevant IT Health Check (ITHC);

(b) for which all issues above an agreed tolerance have been addressed and if needed, retested;

(c) subject to a DPIA

(d) subsequently assured to operate

8.3.5 Development, test, pre-production and user acceptance systems must use non-Real Data. Non-Real Data includes:

(a) Synthetic data.

(b) Anonymised data.

(c) Pseudonymised data.

8.3.6 If anonymisation or pseudonymisation of Real Data into test data is to occur, the risk of re-identification or de-anonymization of test data back into Personal Data must be assessed by the Supplier and communicated to the Authority for review & sign-off. It must not be possible to convert any test data back into real Personal Data by any means, including data matching or dis-aggregation.

8.3.7 Test data must be clearly labelled, and where possible, it should be clear from the format of test data that it is not 'real' to avoid confusion.

8.3.8 For transfer and storage of Bulk Data, the Supplier must apply the NCSC Bulk Data Protection guidance - https://www.ncsc.gov.uk/collection/protecting-bulk-personal-data.

8.3.9 The Supplier shall not delete or remove any proprietary notices contained within or relating to the Authority Data.

8.3.10 The Supplier shall not store, copy, disclose, or use the Authority Data except as necessary for the performance by the Supplier of its obligations under this Contract or as otherwise expressly authorised in writing by the Authority.

8.3.11 To the extent that Authority Data is held and/or processed by the Supplier, the Supplier shall supply that Authority Data to the Authority as requested by the Authority in the format specified.

8.3.12 The Supplier shall take responsibility for preserving the integrity of Authority Data and preventing the corruption or loss of Authority Data that they hold and process.

8.3.13 The Supplier shall perform secure back-ups of all Authority Data and shall ensure that up-to-date back-ups are stored off-site in accordance with the Business Continuity and Disaster Recovery Plan. The Authority shall ensure that such back-ups are available to the Authority at all times upon request.

8.3.14 The Supplier shall ensure that any system on which the Supplier holds any Authority Data, including back-up data, is a secure system that complies with the requirements of this Schedule.

8.3.15 If the Authority Data is corrupted, lost or sufficiently degraded as a result of the Supplier's Default so as to be unusable, the Authority may:

(a) require the Supplier (at the Supplier's expense) to restore or procure the restoration of Authority Data to the extent and in accordance with the requirements specified; and/or

(b) itself restore or procure the restoration of Authority Data and shall be repaid by the Supplier any reasonable expenses incurred in doing so to the extent and in accordance with the requirements specified.

8.4 The following requirements related to data encryption at rest and in transit apply:

8.4.1 The Supplier must carry out risk assessments for all systems to confirm the exact needs for protection of data at rest and data in transit, to identify proportionate controls and where necessary justify variances against the default position. This risk assessment must be communicated to the Authority.

(a) Redacted

8.4.2 The Supplier must ensure that information assets are protected by encryption when in transit between solution integration points to external parties, or between sensitive components (e.g. database connections). Encryption between internal components should be applied if required.

8.4.3 The Supplier must inform the Authority of any encrypted information intended to leave the UK. The Supplier shall ensure that protections, regulations and restrictions that might apply in the relevant part of the world are followed. The Authority must be notified and sign off on any data leaving the UK.

8.4.4 Data must be protected by encryption controls suitable for Official Level data classification

8.4.5 Redacted

8.4.6 The Supplier must establish implement key management system(s) to secure and manage keys throughout their lifetime. The lifecycle of a key includes:

(a) Generation for different systems and applications;

(b) Issuing and obtaining public key certificates;

(c) Distribution to authorised entities;

(d) Storage and access;

(e) Changing and updating keys;

(f) Dealing with compromised keys;

(g) Revoking keys that are compromised or have reached end of use;

(h) Recovering lost or corrupted keys;

(i) Backing up or archiving keys;

(j) Destroying keys.

8.4.7 The key management system should also include training in the use of cryptographic materials and a logging and auditing process of all key management related activities.

8.4.8 The Supplier shall only use encrypted Removable Media in connection with delivery of their obligations under the Contract when agreed with the Authority when connected to the Core Information Management System and alluse must be in strict accordance with the rules about sensitivity and risks of information. In particular, encrypted memory sticks may only be used for datamarked up to and including the Protective Marking of OFFICIAL - SENSITIVE.

8.4.9 All losses of data must be reported to the Authority as soon as possible so that risk mitigation action can be taken. Any theft of Removable media must be reported to the Police and a crime/incident number obtained.

8.5 The following requirements related to data retention, disposal and clear desks apply:

8.5.1 The Supplier must treat all evidence of key business decisions or actions with the Authority as a record.

8.5.2 The Supplier must apply Records Management requirements to its Content Management Procedures in relation to any Authority-related information.

8.5.3 The Supplier must only process data on applications and in file stores approved by the Authority.

8.5.4 The Supplier must label and handle records in accordance with the Government Security Classifications 2018 (or it's successors), see https://www.gov.uk/government/publications/government-security-classifications.

8.5.5 The Supplier must ensure records contain sufficient descriptive information (metadata) to enable indexing and searching of records.

8.5.6 The Supplier must only hold records on IT systems assured to HMG standards, with the capability to be exported to common formats and security appropriate to the security classification of the held assets. Any exceptions to this requirement must be approved by the Authority.

8.5.7 All records in all formats must be stored securely and made accessible to those with appropriate authority.

8.5.8 Any records with a security classification above OFFICIAL-SENSITIVE must be referred to the Authority for advice on how it is to be stored. There is an expectation that the Authority will not have any such records.

8.5.9 Records must only be accessed by individuals with a business need and sufficient security vetting as defined within the Access Control Requirements and Personnel Security Requirements of paragraph 8 of this Annex.

8.5.10 The Supplier must propose a retention and disposal schedule for all records and data items that align with the overall Authority Retention Schedule. The Authority will review and sign off on these schedules.

8.5.11 For guidance on secure storage of any information, especially those with a Government Security Classification above OFFICIAL-SENSITIVE, the Supplier should contact the Authority but must ensure that:

(a) No Authority Data is left unattended;

(b) No Authority Data is left readily accessible or visible;

(c) Desks and printers are clear of all the Authority Data at the close of each business day;

(d) Authority Data that is no longer required is appropriately destroyed or kept securely until it can be securely disposed of in the secure waste at an Authority-approved site;

(e) Core Information Management System devices are logged off or screens locked when they are unattended or not in use, and re-authenticated when users wish to continue using them;

(f) Core Information Management System portable devices (e.g. Laptops, iPads, etc.) are suitably secure when not required or in use;

(g) Core Information Management System portable devices are suitably protected to address privacy when in use (such as the use of a privacy screen).

8.5.12 The Supplier must provide sufficient and appropriate facilities to enable users to store the Authority information securely.

8.6 Redacted

8.7 The following requirements related to authentication apply:

8.7.1 The Supplier must employ suitable authentication mechanisms across all systems within the scope of the Supplier System.

8.7.2 The Supplier must ensure that administrator users use multi-factor authentication to access assets (including Authority Data) within the Supplier System.

8.8 The following requirements related to authorisation apply:

8.8.1 The Supplier must ensure that access to information assets is limited to authorised Supplier staff and contractors on the basis of business need.

8.8.2 The Supplier must ensure that access to its other ICT assets (e.g. connection to the Internet, telephones, mobile phones etc.) is limited to authorised Supplier staff and contractors on the basis of business need.

8.8.3 The Suppler must ensure that access to personal information, particularly information which is the subject to the Data Protection Act, is well controlled.

8.8.4 The Supplier must ensure that its most sensitive information assets are subject to a strict need-to-know policy.

8.8.5 The Supplier must support the Authority in collation of management information statistics for publication.

8.8.6 The Supplier must implement access control mechanisms in line with Protective Monitoring requirements and in a manner that can hold users accountable for their actions.

8.8.7 The Supplier must establish and implement user controls on the immediate installation of software on Supplier ICT systems.

8.8.8 The Supplier must monitor all access to its information assets and ICT facilities.

8.9 The following requirements related to secure development apply:

8.9.1 All systems that the Supplier uses must be acquired or developed in accordance with NCSC Secure Development Principles. See https://www.ncsc.gov.uk/collection/developers-collection/principles.

8.9.2 Where the Supplier develops its own systems or sub-contracts the development of new systems, the Supplier must ensure that:

(a) Principles for engineering secure systems will be established, documented, maintained and applied to any information system implementation efforts.

(b) Information security-related requirements that satisfy the secure systems principles will be included in the requirements for new information systems acquired or developed.

(c) The Supplier will carry out development within a secure environment and protect development and test data as appropriate.

8.9.3 The Supplier shall continuously evaluate security functionality during system development and implementation.

8.9.4 The Supplier must ensure that it only engages secure and assured developers with appropriate minimum security credentials and trained in secure development practices. This requirement applies to all Supplier sub-contractors.

8.10 Redacted

8.11 management apply:

8.11.1 The Supplier must ensure that all products undergo a reasonable and proportionate degree of scrutiny with regards to their security (historical vulnerabilities, time to fix etc).

8.11.2 The Supplier must ensure that any product's security functionality is:

(a) Well aligned with the Authority security requirements and do not undermine other the Authority security features;

(b) Appropriate for the business function they address;

(c) Proportionate for the business function they address.

8.11.3 The Supplier must ensure that it procures ICT systems and services only from secure, reliable suppliers.

8.11.4 Where the Supplier procures systems from external developers and suppliers it must ensure that such developers and suppliers adhere to secure development standards consistent with NCSC Secure Development Standards.

8.11.5 The Supplier must conform to HMG guidance, particularly the Cloud Security Collection. See .https://www.ncsc.gov.uk/collection/cloud-security

8.11.6 The Supplier must ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

8.11.7 The Supplier must ensure that information security is designed and implemented within the development lifecycle of information systems.

8.11.8 The Supplier must ensure the protection of data used for testing.

8.11.9 The Supplier must ensure that third party organisations undertaking development and implementation work shall be subject to the requirements of Annex 1.

8.12 The following requirements related to service administration apply:

8.12.1 All user accounts (including administrator accounts) must satisfy robust requirements for authentication including:

(a) Meet NCSC password complexity requirements. See https://www.ncsc.gov.uk/collection/passwords/updating-your-approach.

(b) Multi-factor authentication enforcement for all administrator access.

8.12.2 A unique administrator account must be used by each designated individual.

8.12.3 Administrators must not share accounts.

8.12.4 Administrators must not share passwords across accounts.

8.12.5 Administrator accounts must only be used for system administration purposes requiring enhanced privileges. Any other activity must be performed from a standard user account.

8.12.6 Service accounts shall not share passwords.

8.12.7 All default passwords must be changed in line with NCSC password policy. See https://www.ncsc.gov.uk/collection/passwords/updating-your-approach.

8.12.8 Each service account which is needed to run software must be uniquely associated with a single identified system administrator.

8.12.9 Accounts must only be issued when subject to an auditable approvals process.

8.12.10 The person issuing the approval for administrator account must also be held responsible for the actions undertaken on the account.

8.12.11 Accounts must be created with the least number of permissions required to perform the intended role.

8.12.12 All accounts must be regularly reviewed and excessive permissions revoked.

8.12.13 Unneeded or generic accounts must be disabled.

8.12.14 Auditable procedures must be implemented to control the issue of access credentials (passwords, tokens etc.) to individuals (including privileged users)

8.12.15 Access control and audit functions must encompass all actions performed interactively on the Supplier System are reliably associated with identifiable individual accounts.

8.12.16 All actions performed by an administrator account must be logged in an immutable manner and subject to independent review for the following actions:

(a) obtaining access to an individual's computer credentials;

(b) bypassing user access restrictions to access, modify or delete an individual's ICT resources.

8.12.17 Accounts must be disabled when a user ceases to be employed by the Supplier or no longer has a business need to use the account.

8.12.18 If a temporary administrator account has been provisioned and used by a third party (for example, an engineer with a repair task), then upon completion and closure of the account, a full review of the collected logs must be undertaken and if necessary, remedial action taken.

8.13 The following requirements related to external interfaces apply:

8.13.1 The Supplier must perform and maintain a risk assessment of its networks.

8.13.2 The Supplier must monitor its networks for performance, capacity and security issues in line with the Protective Monitoring requirement.

8.13.3 The Supplier must periodically review all aspects of security in its networks and adjust the management and control of them as needed.

8.13.4 The Supplier must identify and include in network service agreements, any security measures, service levels and management requirements for all relevant network services.

8.13.5 The Supplier must separate information systems into more manageable groups by dividing large networks into domains. This requirement also applies to any

third party networks or services under the control of (directly or contractually) and used by the Authority.

8.13.6 Any network facilitating non-business use (guest access), must have no access to the Supplier System.

8.13.7 The Supplier must protect each wireless network where present with best-practice security protocols (e.g. WPA2) and a secure password.

8.13.8 The Supplier must implement suitable filtering, auditing and monitoring on all wireless networks.

8.13.9 The Supplier must disable any WPS feature in its networks.

8.13.10 The Supplier must ensure that all wireless access points and associated infrastructure are given appropriate physical protections.

8.13.11 Users should be made aware that:

(a) Their use of Supplier wireless networks should be for business use only (except where separate guest networks are provided);

(b) Guest access is offered as a complimentary service to facilitate their visit to the Supplier System.

(c) The use of Supplier System wireless networks should not bring the Authority into disrepute and must comply with the Annex 1 requirements.

8.14 The following requirements related to data backup apply:

8.14.1 The Supplier must securely backup all software, configurations and system images (including Real Data) on a regular basis.

8.14.2 The Supplier must store these backups in a secondary location to avoid potential damage from a disaster at the prime site.

8.14.3 The Supplier must identify, implement, monitor and update as needed, an appropriate range of technical, physical, procedural and personnel controls over information that is backed up.

8.14.4 The Supplier must maintain and refresh the media of backup data, especially if it is intended to be stored over a large period of time.

8.14.5 The Supplier must regularly test that the information can be retrieved from the backups successfully and within expected timescales.

8.14.6 The Supplier must be able to restore data to the Production environment within expected timescales.

8.14.7 The Supplier must consider the need for operational snapshots of systems and information for long-term storage and make appropriate functional and assurance arrangements as part of the backup regime.

8.14.8 The Supplier must ensure that information backups conform to data retention requirements so that data is not retained beyond the defined limits.

8.15 The following requirements related to incident management apply:

8.15.1 The Supplier must have an incident handling approach that is able to align with the Authority's extant processes. The Supplier must ensure that any necessary people, data and systems are made available to the Authority to support the handling, resolution and investigation of an incident. An incident is any event or action that breaches information security policies and procedures or which compromises, or threatens to compromise, the confidentiality, integrity or availability of information, assets, the communications infrastructure or IT equipment. Incidents include, but aren't limited to:

(a) breaches of physical security;

(b) detection or introduction of malicious code;

(c) inappropriate content;

(d) inappropriate or unauthorised access of IT services or information;

(e) malfunctions of software;

(f) misuse of information, items and/or equipment;

(g) theft or loss of information, items and/or equipment;

(h) unauthorised destruction of information;

(i) unauthorised disclosure of information;

(j) uncontrolled system changes;

(k) unsecure information, items and/or equipment;

(l) violations of network and system access;

(m) unexpected lack of availability to Personal Data related assets.

8.15.2 The Supplier must inform the Authority within 1 hour of observing an incident (including weekends and weekdays, public holidays).

8.15.3 The Supplier must assist the Authority in determining and implementing measures and processes to handle an incident. The final say on mitigation approach rests with the Authority. The Authority will assess incidents and determine if they are to be classified as near misses, security weaknesses or incidents and what actions, if any, are to be taken to mitigate them.

8.15.4 The Authority will record details of incidents, and from these records, prepare periodic reports for management on the nature of the incidents and any systematic issues that may need to be addressed to reduce the likelihood of future incidents. The Supplier must support and provide the Authority with any information needed to complete the categorisation of incidents, and toprepare periodic reports for management.

8.15.5 The Supplier must support the creation of an incident playbook which provides expected mitigations for anticipated incidents types (e.g. a malware alert). The playbook should define named individuals from the Supplier team who will co-ordinate the incident for the Supplier, with their contact details. The Playbook should be regularly reviewed to ensure that mitigations and contact details are accurate.

8.15.6 The Supplier must be prepared to be involved in Incident Drills, which will simulate an incident occurring. The drill shall test the communication and co-ordination of the incident. The Supplier must support the process of improvement for Incident Handling.

8.15.7 The Supplier must preserve information (log files, audit files, systems etc) that will be used in the event of a legal or disciplinary investigation. Files should be protected, and the chain of evidence preserved by ensuring that only authorised people have the ability to access these files. Suspected machines should be isolated from other Supplier systems, rather than turned off, to preserve forensic information.

8.15.8 The Supplier must ensure that its personnel go through regular mandatory data handling, cyber security awareness, and incident handling training (annually and on joining) to understand what an incident is, and how they should report it using the Supplier's incident handling processes. Training must inform users of good security practices, such as locking their computer, not using untrusted USB devices etc.

8.15.9 Supplier personnel must not discuss or report an incident with anyone except the Authority.

8.15.10 All external communications (e.g. to the media, ICO) for an Incident must be handled or co-ordinated by the Authority.

8.16 The following requirements related to forensic readiness apply:

8.16.1 The Supplier shall maintain a forensic readiness capability.

8.16.2 The Supplier must adhere to "The Principles of Digital Evidence", defined within the ACPO Good Practice Guide for Digital Evidence when undertaking formal forensic investigations. See https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf.

8.16.3 The Authority will oversee all investigations, lead on necessary sanctions and recommend security improvements and policy improvements as needed as the result of any investigation. The Supplier must facilitate forensic investigations, and adopt any improvements as a result of a forensic investigation.

8.17 The following requirements related to vulnerability management apply:

8.17.1 The Supplier must establish and maintain contact with external organisations, such as system vendors and information security organisations for prompt notification of threats, vulnerabilities, and the latest vendor-supplied security patches and advice.

8.17.2 The Supplier must arrange for an IT Health Check for the Supplier System in any of the following circumstances:

(a) Prior to a grant of Authority to Proceed or Authority to Operate (e.g. events where the Supplier System is connected to external systems, loaded with Real Data or prior to live operation);

(b) As part of the Authority Security Assurance process integral to change management. Whenever any change is being planned for an existing IT system that is assessed by the Authority as significantly impacting security, whether it relates to business processes, software, infrastructure or ICT support processes. This includes significant releases in an Agile development.

(c) Periodically, defined by risk, reassessed at 12-month intervals.

8.17.3 The ITHC must be performed by a NCSC Green-light CHECK or CREST approved supplier.

8.17.4 The Supplier must implement continuous vulnerability monitoring and remediation to cover the lifecycle of the project. Specific checks shall be made prior to each release and remediated.

8.17.5 The Supplier must document and share with the Authority, ITHC results and identified vulnerabilities. The Supplier shall ensure that ITHC observations are addressed by either:

(a) Mitigating observations in a timely manner;

(b) Obtaining formal acceptance of the vulnerability by the Authority.

8.17.6 The Supplier must notify, contain and remediate all observations identified in ITHC reports, or otherwise, within a time period dependent on the severity of the vulnerability, and agreed by the Authority.

8.17.7 Supplier staff must report the discovery of a potential technical vulnerability that they identify to the Authority.

8.18 The following requirements related to operational security apply:

8.18.1 The Supplier must establish, document, implement and review a set of operating procedures for all information processing and communication systems, including networks.

8.18.2 The Supplier must ensure the separation of development, testing and operational environments, and implement procedures to ensure that operations to incorrect environments are not possible.

8.18.3 The Supplier must ensure that Disaster Recovery facilities are placed to support the principle of controlled separation from other facilities, where feasible.

8.18.4 Only if it is absolutely necessary should testing of facilities be carried out in a live Production environment, either in part or in its entirety. A full risk

assessment must be undertaken and clearance given by the Authority before such actions are taken.

8.18.5 The Supplier must ensure that any changes are reflected into the Supplier System in a controlled manner, subject to a formal change control process, whether the changes relate to:

(a) business processes;

(b) information processing facilities and systems;

(c) network and communications facilities;

(d) Locations;

(e) Procedures.

8.18.6 The Supplier must maintain system performance by monitoring and tuning resources, and predicting future capacity requirements.

8.18.7 The Supplier must implement controls on any changes to operational Production systems.

8.18.8 The Supplier must levy these operational security requirements on any outsourced or 3rd party suppliers.

8.19 The following requirements related to personnel security apply:

8.19.1 Background verification checks shall be carried out on all prospective staff for employment history and criminal record checks. The checks shall be carried out in accordance with relevant laws and regulations.

8.19.2 All Supplier staff, including prospective staff and contractors, must attain or already hold the relevant security clearance for the work they will be performing for the Authority, before their work commences.

8.19.3 Verification checks must be carried out in accordance with HMG policy. At the time of writing, this is as a minimum the pre-employment checks of BPSS. Disclosure Scotland, DBS AccessNI, National Security Vetting and Non-Police Personnel Vetting (NPPV) clearances may be necessary for more sensitive roles.

8.19.4 The Authority may require existing staff to undergo further verification checks for new roles, prior to, and as a condition of, appointment and acceptance of sensitive new or changed roles. The supplier must facilitate further verification checks.

8.19.5 The Supplier must have a contractual agreement with its contractors and employees which outlines the responsibilities of all parties in respect of the Authority's information security requirements.

8.19.6 The terms and conditions of the employment of staff or contractors working on the Authority assets and with the Authority data must include:

(a) legal responsibilities and rights (e.g. regarding data protection legislation);

(b) responsibilities for the security and maintenance of Authority Data and information processing facilities;

(c) responsibilities for handling information received from external parties and use of third party applications and systems;

(d) responsibilities after termination of employment.;

(e) actions to be taken if Supplier staff or contractors disregard the Supplier information security policy document set or specific controls set out by the Supplier for their staff under their compliance with the Authority's security requirement.

8.19.7 Supplier staff must be periodically made aware, educated and trained in the information security, policies and procedures associated with their role working with the Authority assets and the Authority data.

8.19.8 The Supplier must have a formal and communicated disciplinary process in place to take action against staff and contractors as and when necessary. This includes those persons who have committed an information security breach.

8.20 The following requirements related to physical security apply:

8.20.1 The Supplier must protect with appropriate physical security controls any part of its business, staff, customer information, assets (of all types) and information insofar as they pertain to the Supplier System.

8.20.2 The Supplier must carry out a risk assessment to identify the requirements for specific physical security controls in accordance with these security requirements.

8.20.3 The Supplier shall implement specific physical security controls in accordance with:

(a) the Supplier risk assessment;

(b) the requirements of the Security Policy Framework. See https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework.

(c) the requirements of CPNI guidance on physical security, covering perimeter, within site, buildings and assets. See https://www.cpni.gov.uk/protecting-my-asset.

(d) the guidance of ISO27001 and ISO27002.

8.21 Without prejudice to the provisions relating to audit under Schedules 2.1 (Services Description) and 7.5 (Financial Reports and Audit Rights), the following requirements shall apply to security audit:

8.21.1 The Supplier must facilitate the Authority to carry out audits on its estate where used to directly or indirectly deliver the services to the Authority, or

immediately without prior arrangement in response to a security alert or incident.

8.21.2 Authority audits will be agreed between the Authority and the Supplier, and carefully planned to minimise disruptions to business processes.

8.21.3 All audits should be monitored and logged to produce a reference trail and be reported to the appropriate management.

8.21.4 Specific audits shall be carried out regularly against:

(a) system protective monitoring logs;

(b) the Supplier asset register, particularly: portable ICT equipment; office equipment assets; servers and associated data centre ICT assets; software and software licences;

(c) the Supplier user register and access control permissions, particularly the number and nature of administrator users across the estate;

(d) infrastructure every three months by reviewing: any new independent Audit reports supplied via the service providers covering ISO27001, PCI Compliance, SOC1 & SOC2 scopes; any updates to the suppliers Cloud Security Principles documentation; any Privacy Shield registrations should there be a US connection;

(e) patching records across the Supplier services.

8.21 A The Authority's auditors may from time to time visit the Sites in order to ensure all procedures and requirements and the validation of candidate ID are compliant with this Agreement, are correctly and consistently applied and the integrity of the Services is maintained. Upon presentation of an agreed form of identification, the Supplier shall allow the auditors unrestricted access to the Site and to all documentation and records relating to the delivery of Services without prior notice. For the avoidance of doubt, the Authority's unrestricted access to Sites, information and/or records for audit purposes as outlined in this paragraph 8.21A of Schedule 2.4 shall not include access to information or data maintained by the Supplier for any of the Supplier's other clients or assessment programs that are unrelated to the provision of the Services.

8.22 Without prejudice to the provisions relating to audit under Schedules 2.1 (Services Description) and 7.5 (Financial Reports and Audit Rights), the following requirements shall apply to security review:

8.22.1 The Supplier must periodically review its information security policies and procedures. The reviews should be undertaken:

(a) at planned intervals, not less than annually;

(b) when there is a significant change to the business, networks and systems or threats to the business;

(c) when there has been a significant security incident.

8.22.2 The Authority will audit the Supplier's compliance with the information security policies and procedures on a similar basis. Audits will be carried out by independent personnel and the Supplier shall facilitate this audit.

8.22.3 The Supplier must implement new or amended information security policies and procedures as an outcome of the reviews and audits, if needed.

8.23 The following requirements related to perimeter protection apply:

8.23.1 The Supplier must operate its systems in accordance with HMG Policy and industry best practice for the control of malware, content checking and perimeter control. See also https://www.ncsc.gov.uk/guidance/mitigating-malware.

8.23.2 The Supplier must establish detailed personnel, physical, procedural and technical measures to reduce the risks to the Authority information assets from malware, bad content and to protect the perimeter of its systems.

8.23.3 The Supplier must maintain a risk assessment of the techniques, threats and potential vulnerabilities to its information assets and implement proportionate technical responses, from:

(a) malware;

(b) bad content;

(c) perimeter attacks.

8.23.4 The Supplier must derive from the risk assessment, and in accordance with HMG Policy and industry best practice for security architectures, implement appropriate technical measures to mitigate malware, contain bad content and protect the perimeter of its system from attack.

8.23.5 The Supplier must require all users to report promptly any security incident, including malware attacks, either confirmed or suspected.

8.23.6 The Supplier must provide guidance and training to its users to help them identify social engineering attacks that may accompany malware or perimeter attacks (e.g. phishing, password disclosure, clicking on unknown email attachments etc).

8.23.7 The Supplier must review, update and re-issue user guidance when new attacks become known.

8.23.8 The Supplier must maintain a security architecture for the Suppliers network in accordance with NCSC Architectural Patterns. See https://www.ncsc.gov.uk/collection/cyber-security-design-principles/cyber-security-design-principles and share this with the Authority upon request where this is not directly part of the Assurance Documentation.

8.23.9 The Supplier shall review and update as needed, at least quarterly and also in response to known security incidents and to significant systems and network changes:

(a) the security risk assessment;

(b) the Supplier System security architecture;

(c) the detailed controls required to support this requirement;

(d) the guidance given to users.

8.24 The following requirements related to data transfers apply:

8.24.1 The Authority characterises information transfers as ranging from short-term exchanges of information with partners to strategic long-term data processing arrangements with outsource suppliers. Bulk transfers of data must comply with NCSC Guidance on protecting bulk person data. See https://www.ncsc.gov.uk/collection/protecting-bulk-personal-data.

8.24.2 The Supplier must ensure that all information transfers are carried out under the governance of the Authority.

8.24.3 The Supplier must ensure that all information transfers are carried out in a secure manner to protect the confidentiality of the information, maintain its integrity and maintain appropriate levels of availability.

8.24.4 The Supplier must comply with implementation procedures and controls for the protection of information during transfer, in line with Authority guidance.

8.24.5 The Supplier shall ensure that all information transfers comply with relevant legislation and standards (e.g. Data Protection Act, HMG Security Policy Framework, etc).

8.24.6 The Supplier, when exchanging information with external parties, set out agreements as to how the information can be used and how it will be protected. These agreements must be reviewed and approved by the Authority, which shall include:

(a) responsibilities for audit, control, disposal and decommissioning, governance, management, operation, review and update of CoP and the information;

(b) the necessary controls particular to messaging (e.g. email, electronic data interchange, social networking, etc.);

(c) the necessary controls particular to Data Sharing;

(d) the necessary controls required by data protection legislation, freedom of information legislation and the Authority.

8.24.7 The Suppler may need to complete confidentiality or non-disclosure agreements to enforce the protection of information when transferred either within the Authority or to external parties.

8.25 The following requirements related to certifications apply:

8.25.1 The Supplier must comply with the HMG security policy framework, other policies and guidance in the management of information security such as ISO27001.

8.25.2 The Supplier must maintain an appropriate governance structure in order to effectively manage information security.

8.25.3 The Supplier must maintain proportionate and risk-based, personnel, procedural, technical and physical controls to protect the confidentiality, integrity and availability of its information assets.

8.26 The following requirements related to operation of end user devices apply:

8.26.1 Removable media must be secured and suppliers must comply with NCSC guidance on securing End User Devices. See https://www.ncsc.gov.uk/collection/end-user-device-security/eud-overview/eud-security-principles.

8.26.2 Removable media must not be used to transfer information unless there is a clear business need and no more appropriate, secure, alternate methods exist.

8.26.3 All information transfer via removable media must be approved by the Authority.

8.26.4 The Supplier must maintain a register of all removable media assets. The register shall record at a minimum the location and keeper of the media and a synopsis of the information held on it.

8.26.5 The Supplier must periodically muster the removable media inventory to gain assurance that all assets can be accounted for.

8.26.6 Personal devices must not be physically connected to any the Authority systems (even to charge the device) unless there is a clear business need.

8.26.7 The removable media device or the information on it, shall be encrypted unless there are specific reasons not to.

8.26.8 When considering accessing external media:

(a) media must be scanned for malware before use;

(b) where the Authority agrees specific exceptions, the user must ensure that the equipment (e.g. laptop) has up-to-date and functioning anti-malware software.

8.26.9 Removable media must be locked away or stored securely when not required.

8.26.10 Any loss or theft of removable media must be reported to the Authority immediately.

8.26.11 If any piece of removable media is no longer required, its contents must be erased and made unrecoverable by overwriting or destruction.

8.26.12 Removable media that is to be destroyed must be disposed of in line with the NCSC decommissioning requirements. See https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media.

8.26.13 Where removable media is used for long term storage, the long-term viability of the media must be assessed. Procedures must be put in place to periodically

transfer the information to fresh media to mitigate the risk of information loss through media failure.

8.27 The following requirements related to disposal of end user devices apply:

8.27.1 Supplier System assets shall be subject to decommissioning when:

(a) the business need, which incorporates the asset, ends (e.g. the system is withdrawn);

(b) the service life of the asset is over;

(c) the asset has failed.

8.27.2 All Supplier System assets must be assessed for the need for decommissioning. Items will either:

(a) not need attention (e.g. power supplies);

(b) clearly need attention (e.g. disk drives);

(c) be less obvious (e.g. RAM modules, screens, telephones etc.) but still require attention.

8.27.3 All Supplier-owned assets used in relation to the Supplier System or Supplier Service must be decommissioned in accordance with HMG Information Assurance Standard 5 (IS5), HMG Information Assurance Standard 4 (IS4) Supplement 9 and their successors.

8.27.4 Not used.

8.27.5 Data held on IT assets must be reviewed before decommissioning:

(a) the Authority will decide whether: the data is to be retained in the Authority by migration to other media; or the data is to be deleted;

(b) the Authority will decide what the eventual outcome of the device is to be.

8.27.6 Data held on Supplier System assets that are to be decommissioned must be erased by overwriting or magnetic wiping (degaussing) on-site as soon as possible.

8.27.7 Media that is to be destroyed must be disposed of in line with the NCSC decommissioning requirements. See https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media.

8.27.8 Decommissioning and destruction records and certificates must be created and maintained for all Supplier System assets. Records and certificates must be retained.

8.27.9 The decommissioning policy must also be implemented by any Supplier outsource partners and their successors.

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

(a) securely destroys Authority Data only on Sites which are included within the scope of an existing certification of compliance withISO/IEC 27001:2013;

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

(c) the Supplier must 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) must be permitted to carry out the secure destruction of the Authority Data;

(d) the Supplier must 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, must or must procure that the relevant Sub-contractor must: immediately cease using the Authority Data; and procure that the relevant Sub-contractor promptly returns, destroys and/or erases the Authority Data in accordance with this Annex.

8.28 Redacted

Annex 2

NOT USED

Annex 3

Security Assurance Documentation Template

The Security Assurance Documentation is a collection of artefacts. At the apex of these artefacts is the Security Assurance Document, which summarises the more expansive content of the lower-level artefacts such as the detailed security risk assessment, risk treatment detail, in-service detail such as incident management, and other assurance evidence such as Supplier certification.

Production of separate artefacts supports ease of revision and their staged delivery as necessary. Provision of artefacts within project collaboration tools improves consistency with the wider Supplier deliverables, by using hyperlinks instead of repetition to prevent information staling.

The Security Assurance Document can be seen as an "executive summary" of the wider Security Assurance Documentation which supports the Security Assurance Decision. The summary content is as indicated.

0. Document configuration information

- Change History, including version, date of change, by whom, nature of change and brief reason for change.
- References.
- Dependencies that contain supporting information and assurance.

1. Executive summary

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

2. Functional system description

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

- Background.
- Context with other systems.
- Data assets categories and flows, including volumes.
- User types and numbers.

3. Threats and risk management

<*This section summarises the detailed security risk assessment and should not attempt to identify all risks and their means of risk treatment. Instead, provide a more qualitative summary in business language, covering risks to confidentiality, integrity and availability.*>

- Key threats.

- Key impacts.
- Main risks.

4. Security requirements

<*This section summarises security requirements particular to the Information Management System, i.e. beyond minimum standards and best practices.*>

5. Solution architecture

<*This section provides a high-level view of the solution, using diagrams to convey most of the information.*>

- Architecture (technical and physical) of the operational system.
- Architecture (technical and physical) of the means of delivery of the operational system.
- Architecture (technical and physical) of the service design for the operational system.

6. Security architecture - technical

<*This section summarises the technical security controls applied throughout the system, in terms of the contribution of architectural approaches, the application of "minimum standards", and the treatment of specific requirements. Applies to delivered system, its means of delivery and the means of its operation.*>

- Architectural overview, including relevant patterns.
- Constraints and limitations.
- Overview of security controls.

7. Security architecture - non-technical

<*This section summarises the non-technical security controls applied throughout the system, in terms of the personnel, physical and procedural controls.* >

- Personnel controls.
- Physical controls.
- Procedural controls (including any security operating procedures),

8. Security testing

<*A summary of security testing in the form of ITHC events performed.*>

- A tabulation of ITHC events including the date, the organisation undertaking the health check, a summary of the scope of the event, and a summary of the findings and the highest-ranked finding.

9. Residual risks

<*A summary of the residual risks which are likely to be above the stated risk appetite after all controls have been applied and verified.*>

- A tabulation of residual risks including a description of the risk, its severity, its action status (whether it should be accepted, treated or has not yet been determined) and supporting comments including timescales where appropriate.

- References to security backlogs.

- Reference to end-of-life information.

10. Index of supporting material

<*References to the main artefacts summarised in the Security Assurance Document and any other relevant items. Usually those artefacts at the next level in the evidential pyramid.*>