Schedule 6

Security

(Call-Off Schedule 9)

Schedule 6 Security

Definitions

1.1 In this Schedule the following words shall have the following meanings:

"Asset"	any item or equipment owned by the *Client* or a Business Unit which is maintained by the *Service Provider* as part of the *service;*
"Baseline Security Requirements"	the requirements set out in Annex 1 to this Schedule;
"Commercial off the shelf Software" or "COTS Software"	non-customised software where the IPR may be owned and licensed either by the *Service Provider* or a third party depending on the context, and which is commercially available for purchase and subject to standard licence terms;
"Breach of Security"	means the occurrence of: a) any unauthorised access to or use of the *service*, the Affected Property and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the *Client* and/or the *Service Provider* in connection with this contract; and/or b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the *Client* and/or the *Service Provider* in connection with this contract, in either case as more particularly set out in the security requirements in the Security Policy where the *Client* has required compliance therewith in accordance with paragraph 3.4.3(d) of this Schedule;
"Client System"	the *Client's* computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the *Client* or the *Service Provider* in connection with this contract which is owned by or licensed to the *Client* by a third party and which interfaces with the Service Provider System or which is necessary for the *Client* to receive the s*ervice*;

"ICT Environment"	the Client System and the Service Provider System;
“ICT Policy”	the *Client’s* policy in respect of information and communications technology in force as at the Contract Date (a copy of which has been supplied to the *Service Provider*), as updated from time to time and notified to the *Service Provider*;
“IPR”	any and all patents, trademarks, service marks, copyright, moral rights, rights in a design, know-how, Confidential Information and all or any other intellectual or industrial property rights whether or not registered or capable of registration and whether subsisting in the United Kingdom or any other part of the world together with all or any goodwill relating or attached thereto;
"ISMS"	the information security management system and process developed by the *Service Provider* in accordance with paragraph 3 (ISMS) as updated from time to time in accordance with this Schedule;
“Security Policy”	the *Client's* security policy in force as at the Contract Date (a copy of which has been supplied to the *Service Provider*), as updated from time to time and notified to the *Service Provider*;
"Security Tests"	tests to validate the ISMS and security of all relevant processes, systems, incident response plans, patches to vulnerabilities and mitigations to Breaches of Security;
“Service Provider System”	the information and communications technology systems used by the *Service Provider* in supplying the *service*, including the COTS Software, the *Service Provider’s* equipment, configuration and management utilities, calibration and testing tools and related cabling (but excluding the Client System) including all modifications and enhancements and upgrades;

2. Security Requirements

2.1 The Parties acknowledge that the purpose of the ISMS and Security Management Plan are to ensure a good organisational approach to security under which the specific requirements of this contract will be met.

2.2 The Parties shall each appoint a security representative to be responsible for Security. The initial security representatives of the Parties are:

2.2.1 *Client:* [redacted], Head of Cyber and Information Security

2.2.2 *Service Provider:* [redacted] IT Security Officer and Security Controller

2.3 The *Client* shall clearly articulate its high-level security requirements in writing so that the *Service Provider* can ensure that the ISMS, security related activities and any mitigations are driven by these fundamental needs.

2.4 Both Parties shall provide a reasonable level of access to any members of their staff for the purposes of designing, implementing and managing security.

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

2.6 The *Service Provider* shall ensure the up-to-date maintenance of a security policy relating to the operation of its own organisation and systems and on request shall supply this document as soon as practicable to the *Client* security representative.

2.7 The *Client* and the *Service Provider* acknowledge that information security risks are shared between the Parties and that a compromise of either the *Service Provider* or the *Client's* security provisions represents an unacceptable risk to the *Client* requiring immediate communication and co-operation between the Parties.

3. Information Security Management System (ISMS)

3.1 The *Service Provider* shall develop and submit to the *Client* security representative, within twenty (20) Working Days after the Contract Date, an information security management system for the purposes of this contract and shall comply with the requirements of paragraphs 3.4 to 3.6.

3.2 The *Service Provider* acknowledges that the *Client* places great emphasis on the reliability of the performance of the *service*, confidentiality, integrity and availability of information and consequently on the security provided by the ISMS and that the *Service Provider* shall be responsible for the effective performance of the ISMS.

3.3 The *Client* acknowledges that;

3.3.1 If the *Client* has not stipulated that it requires a bespoke ISMS, the ISMS provided by the *Service Provider* may be an extant ISMS covering the *service* and their implementation across the *Service Provider's* estate; and

3.3.2 Where the *Client* has stipulated that it requires a bespoke ISMS then the *Service Provider* shall be required to present the ISMS for the *Client* security representative's acceptance.

3.4 The ISMS shall:

3.4.1 be developed to protect all aspects of the *service* and all processes associated with the provision of the *service*, including the Client's premises, the Affected Property, the Service Provider System, the Client System (to the extent that it is under the control of the *Service Provider*) and any ICT, information and data (including the *Client's* Confidential Information and the Government Data) to the extent used by the *Client* or the *Service Provider* in connection with this contract;

3.4.2 meet the relevant standards in ISO/IEC 27001 and ISO/IEC27002 in accordance with paragraph 7;

3.4.3 at all times provide a level of security which:

a) is in accordance with the Law and this contract;

b) complies with the Baseline Security Requirements set out in Annex 1 to this Schedule;

c) as a minimum demonstrates Good Industry Practice;

d) complies with the Security Policy and the ICT Policy;

e) complies with at least the minimum set of security measures and standards as determined by the Security Policy Framework (Tiers 1-4) available at(https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework)

f) takes account of guidance issued by the Centre for Protection of National Infrastructure available at (https://www.cpni.gov.uk)

g) complies with HMG Information Assurance Maturity Model and Assurance Framework available at (https://www.ncsc.gov.uk/articles/hmg-ia-maturity-model-iamm)

h) meets any specific security threats of immediate relevance to the ISMS, the *service* and/or Government Data;

i) addresses issues of incompatibility with the *Service Provider's* own organisational security policies; and

j) complies with ISO/IEC27001 and ISO/IEC27002 in accordance with paragraph 7;

3.4.4 document the security incident management processes and incident response plans;

3.4.5 document the vulnerability management policy including processes for identification of system vulnerabilities and assessment of the potential impact on the *service* of any new threat, vulnerability or exploitation technique of which the *Service Provider* becomes aware, prioritisation of security patches, testing of security patches, application of security patches, a process for *Client* security representative acceptances of

exceptions, and the reporting and audit mechanism detailing the efficacy of the patching policy; and

3.4.6 be certified by (or by a person with the direct delegated authority of) a *Service Provider's* main board representative, being the "Chief Security Officer", "Chief Information Officer", "Chief Technical Officer" or "Chief Financial Officer" (or equivalent as agreed in writing by the *Client* security representative in advance of issue of the relevant Security Management Plan).

3.5 Subject to paragraph 2 the references to standards, guidance and policies contained or set out in paragraph 3.4 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the *Service Provider* from time to time.

3.6 In the event that the *Service Provider* becomes aware of any inconsistency in the provisions of the standards, guidance and policies set out in paragraph 3.4, the *Service Provider* shall immediately notify the *Client* security representative of such inconsistency and the *Client* security representative shall, as soon as practicable, notify the *Service Provider* as to which provision the *Service Provider* shall comply with.

3.7 If the bespoke ISMS submitted to the *Client* security representative pursuant to paragraph 3.3.1 is accepted by the *Client* security representative, it shall be adopted by the *Service Provider* immediately and thereafter operated and maintained in accordance with this Schedule. If the ISMS is not accepted by the *Client* security representative, the *Service Provider* shall amend it within ten (10) Working Days of a notice of non-acceptance from the *Client* security representative and re-submit it for acceptance. The Parties shall use all reasonable endeavours to ensure that the acceptance process takes as little time as possible and, in any event, no longer than fifteen (15) Working Days from the date of the first submission of the ISMS to the Client security representative. If the *Client* security representative does not accept the ISMS following its resubmission, the matter shall be resolved in accordance with clause 90 of the contract. No acceptance to be given by the *Client* security representative pursuant to this paragraph 3 may be unreasonably withheld or delayed. However, any failure to accept the ISMS on the grounds that it does not comply with any of the requirements set out in paragraphs 3.4 to 3.6 shall be deemed to be reasonable.

3.8 Acceptance by the *Client* security representative of the ISMS pursuant to paragraph 3.7 or of any change to the ISMS shall not relieve the *Service Provider* of its obligations under this Schedule.

4. Security Management Plan

4.1 Within the *period for reply* after the Contract Date, the *Service Provider* shall prepare and submit to the *Client* security representative for acceptance in accordance with paragraph 4 fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of paragraph 4.2.

4.2 The Security Management Plan shall:

4.2.1 be based on the initial Security Management Plan set out in Annex 2 (Security Management Plan) to this Schedule;

4.2.2 comply with the 'Baseline Security Requirements' set out in Annex 1 to this Schedule, the Scope, and, where specified by the *Client* in accordance with paragraph 3.4.3(d), the Security Policy;

4.2.3 identify the necessary delegated organisational roles defined for those responsible for ensuring this Schedule is complied with by the *Service Provider*;

4.2.4 detail the process for managing any security risks from Subcontractors, Others and third parties authorised by the *Client* with access to the *service*, processes associated with the delivery of the *service*, the Affect Property, the Service Provider System, the Client System (to the extent that it is under the control of the *Service Provider*) and any ICT, Information and data (including the *Client's* Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that information, data and/or the *service*;

4.2.5 unless otherwise specified by the *Client* security representative in writing, be developed to protect all aspects of the *service* and all processes associated with the delivery of the *service*, including the Affected Property, the Service Provider System, the Client System (to the extent that it is under the control of the *Service Provider*) and any ICT, Information and data (including the *Client's* Confidential Information and the Government Data) to the extent used by the *Client* or the *Service Provider* in connection with this contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the *service*;

4.2.6 set out the security measures to be implemented and maintained by the *Service Provider* in relation to all aspects of the *service* and all processes associated with the delivery of the *service* and at all times comply with and specify security measures and procedures which are sufficient to ensure that the *service* comply with the provisions of this Schedule (including the requirements set out in paragraph 3.4) and the Scope;

4.2.7 demonstrate that the *Service Provider's* approach to delivery of the *service* has minimised the *Client* and *Service Provider* effort required to comply with the Scope and this Schedule through consideration of available, appropriate and practicable pan-government accredited services (for example, 'platform as a service' offering from the UK Government's 'G-Cloud' catalogue);

4.2.8 set out the plans for transitioning all security arrangements and responsibilities from those in place at the Contract Date to those incorporated in the ISMS within the timeframe agreed between the Parties;

4.2.9 set out the scope of the Client System that is under the control of the *Service Provider*;

4.2.10 be structured in accordance with ISO/IEC27001 and ISO/IEC27002, cross-referencing if necessary to other provisions in the contract which cover specific areas included within those standards; and

4.2.11 be written in plain English in language which is readily comprehensible to the staff of the *Service Provider* and the *Client* and shall reference only documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule and/or the Scope.

4.3 The *Service Provider* provides a Security Management Plan or revised Security Management Plan annually or as requested by the *Client* security representative, within the period for reply for acceptance. The *Service Provider* provides information required by the Scope and this Schedule in the Security Management Plan. If the submitted Security Management Plan does not comply with the Scope, Schedule, the Accepted Plan or does not allow the *Service Provider* to Provide the Service the *Client* security representative will instruct the *Service Provider* to submit a revised Security Management Plan.

4.4 Acceptance by the *Client* security representative of the Security Management Plan shall not relieve the *Service Provider* of its obligations to deliver the *service*.

5. Amendment of the ISMS and Security Management Plan

5.1 The ISMS and Security Management Plan shall be fully reviewed and updated by the *Service Provider* and at least annually to reflect:

5.1.1 emerging changes in Good Industry Practice;

5.1.2 any change or proposed change to the Service Provider System, the *service* and/or associated processes;

5.1.3 any new perceived or changed security threats;

5.1.4 where required in accordance with paragraph 3.4.3(d), any changes to the Security Policy;

5.1.5 any new perceived or changed security threats; and

5.1.6 any reasonable change in requirement requested by the *Client* security representative.

5.2 The *Service Provider* shall provide the *Client* security representative with the results of such reviews as soon as reasonably practicable after their completion and amend the ISMS and Security Management Plan at no additional cost to the *Client*. The results of the review shall include, without limitation:

5.2.1 suggested improvements to the effectiveness of the ISMS;

5.2.2 updates to the risk assessments;

5.2.3 proposed modifications to the procedures and controls that affect information security to respond to events that may impact on the ISMS; and

5.2.4 suggested improvements in measuring the effectiveness of controls.

5.3 Subject to paragraph 5.4, any material change which the *Service Provider* proposes to make to the ISMS or Security Management Plan (as a result of a review carried out pursuant to paragraph 5.1, a *Client* request, a change to Annex 1 (Security) or otherwise) shall be subject to clause 16.

5.4 The *Client* may, acting reasonably, accept and require changes or amendments to the ISMS or Security Management Plan to be implemented on timescales faster than set out in the Scope but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to clause 16 for the purposes of formalising and documenting the relevant change or amendment.

6. Security Testing

6.1 The *Service Provider* shall conduct Security Tests from time to time (and at least annually across the scope of the ISMS) and additionally after any change or amendment to the ISMS (including security incident management processes and incident response plans) or the Security Management Plan. Security Tests shall be designed and implemented by the Service Provider so as to minimise the impact on the delivery of the *service* and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the *Client* security representative. Subject to compliance by the *Service Provider* with the foregoing requirements, if any Security Tests adversely affect the *Service Provider's* ability to deliver the *service* so as to meet the KPIs, and where agreed with the *Client* security representative in advance, the *Service Provider* shall be granted relief against any resultant under-performance for the period of the Security Tests.

6.2 The *Client* shall be entitled to send a representative to witness the conduct of the Security Tests. The *Service Provider* shall provide the *Client* security representative with the results of such Security Tests (in a form accepted by the *Client* security representative in advance) as soon as practicable after completion of each Security Test.

6.3 Without prejudice to any other right of audit or access granted to the *Client* pursuant to this contract, the *Client* and/or its authorised representatives shall be entitled, at any time upon giving reasonable notice to the *Service Provider*, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the *Service Provider's* compliance with the ISMS and the Security Management Plan. The *Client* security representative may notify the *Service Provider* of the results of such tests after completion of each such test. If any such *Client's* test adversely affects the *Service Provider's* ability to deliver the *service* so as to meet the KPIs, the *Service Provider* shall be granted relief against any resultant under-performance for the period of the *Client's* test.

6.4 Where any Security Test carried out pursuant to paragraphs 6.2 or 6.3 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the *Service Provider* shall promptly notify the *Client* of any changes to the ISMS and to the Security Management Plan or other related plan/incident management plan/procedure/process (and the implementation thereof) which the *Service Provider* proposes to make in order to correct such failure or weakness. Subject to the *Client's* prior written acceptance, the *Service Provider* shall implement such changes to the ISMS and the Security Management Plan and repeat the

relevant Security Tests in accordance with the timetable agreed with the *Client* security representative or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan is to address a non-compliance with the Security Policy or security requirements (as set out in Annex 1 (Baseline Security Requirements) to this Schedule) or the requirements of this Schedule, the change to the ISMS or Security Management Plan shall be at no cost to the *Client*.

6.5 If any repeat Security Test carried out pursuant to paragraph 6.4 reveals an actual or potential Breach of Security exploiting the same root cause failure this shall be a substantial failure by the *Service Provider* to comply with its obligations under the contract.

7. Complying with the ISMS

7.1 The *Client* shall be entitled to carry out such security audits as it may reasonably deem necessary in order to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001 and/or the Security Policy where such compliance is required in accordance with paragraph 3.4.3(d).

7.2 If, on the basis of evidence provided by such security audits, it is the *Client's* reasonable opinion that compliance with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy are not being achieved by the *Service Provider*, then the *Client* security representative shall notify the *Service Provider* of the same and give the *Service Provider* a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to implement and remedy. If the *Service Provider* does not become compliant within the required time then the *Client* shall have the right to obtain an independent audit against these standards in whole or in part.

7.3 If, as a result of any such independent audit as described in paragraph 7.1 the *Service Provider* is found to be non-compliant with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy then the *Service Provider* shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the *Client* in obtaining such audit.

8. Security Breach

8.1 Either Party shall notify the other within 1 hour of a breach being identified in accordance with the agreed security incident management process as defined by the ISMS upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.

8.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in paragraph 8.1, the *Service Provider* shall:

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

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

b) remedy such Breach of Security or any potential or attempted Breach of Security in order to protect the integrity of the Affected Property and/or *Client's* Assets and/or ISMS to the extent that this is within the *Service Provider's* control;

c) apply a tested mitigation against any such Breach of Security or attempted Breach of Security and provided that reasonable testing has been undertaken by the *Service Provider*, if the mitigation adversely affects the *Service Provider* ability to Provide the Service so as to meet the relevant KPIs, the *Service Provider* shall be granted relief against any resultant under-performance for such period as the *Client*, acting reasonably, may specify by written notice to the *Service Provider*;

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

e) supply any requested data to the *Client* (or the 'Computer Emergency Response Team for UK Government' ("GovCertUK")) on the *Client's* request within two (2) Working Days and without charge (where such requests are reasonably related to a possible incident or compromise); and

f) as soon as reasonably practicable provide to the *Client* security representative full details (using the reporting mechanism defined by the ISMS) of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the *Client*.

8.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the ISMS with the Security Policy (where relevant) or the requirements of this Schedule, then any required change to the ISMS shall be at no cost to the *Client*.

9. Vulnerabilities and fixing them

9.1 The *Client* and the *Service Provider* acknowledge that from time to time vulnerabilities in the ICT Environment will be discovered which unless mitigated will present an unacceptable risk to the *Client's* information.

9.2 The severity of threat vulnerabilities for COTS Software shall be categorised by the *Service Provider* as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the agreed method in the ISMS and using the appropriate vulnerability scoring systems including:

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

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

9.3 The *Service Provider* shall procure the application of security patches to vulnerabilities within a maximum period from the public release of such patches with those vulnerabilities categorised as 'Critical' within 10 Working Days of release, 'Important' within 20 Working Days of release and all 'Other' within 60 Working Days of release, except where:

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

9.3.2 the application of a 'Critical' or 'Important' security patch adversely affects the *Service Provider's* ability to deliver the *service* in which case the *Service Provider* shall be granted an extension to such timescales of 2 Working Days, provided the *Service Provider* had followed and continues to follow the security patch test plan agreed with the *Client* security representative; or

9.3.3 the *Client* agrees a different maximum period after a case-by-case consultation with the *Service Provider* under the processes defined in the ISMS.

9.4 The *Service Provider* shall use the major version upgrades of all COTS Software within 6 months of the release of the latest version, such that the *Service Provider* uses COTS Software of no older than one major version level below the latest release (normally codified as running software no older than the 'n-1 version') throughout the *Service Period* unless:

9.4.1 where upgrading such COTS Software reduces the level of mitigations for known threats, vulnerabilities or exploitation techniques, provided always that such upgrade is made within 12 months of release of the latest version; or

9.4.2 is agreed with the *Client* in writing.

9.5 The *Service Provider* shall:

9.5.1 implement a mechanism for receiving, analysing and acting upon threat information supplied by GovCertUK, or any other competent central government body;

9.5.2 ensure that the ICT Environment (to the extent that the ICT Environment is within the control of the *Service Provider*) is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

9.5.3 ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the ICT Environment by actively monitoring the threat landscape during the Service Period;

9.5.4 pro-actively scan the ICT Environment (to the extent that the ICT Environment is within the control of the *Service Provider*) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS as developed under paragraph 3.3.5;

9.5.5 from the date specified in the Security Management Plan provide a report to the *Client* security representative within five (5) Working Days of the end of each month detailing both patched and outstanding vulnerabilities in the ICT Environment (to the extent that the ICT Environment is within the control of the *Service Provider*) and any elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report;

9.5.6 propose interim mitigation measures to vulnerabilities in the ICT Environment known to be exploitable where a security patch is not immediately available;

9.5.7 remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the *service* (in order to reduce the attack surface of the ICT Environment); and

9.5.8 inform the *Client* security representative when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the ICT Environment and provide initial indications of possible mitigations.

9.6 If the *Service Provider* is unlikely to be able to mitigate the vulnerability within the timescales under this paragraph 9, the Service Provider shall immediately notify the *Client* security representative.

9.7 A failure by the *Service Provider* to comply with paragraph 9.3 shall constitute a Service Failure.

Annex 1:

Baseline security requirements

1. Handling Classified information

1.1 The *Service Provider* shall not handle *Client* information classified SECRET or TOP SECRET except if there is a specific requirement and in this case prior to receipt of such information the *Service Provider* shall seek additional specific guidance from the *Client* security representative.

2. End user devices

2.1 When Government Data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or system component which has been formally assured through a recognised certification process of the National Cyber Security Centre ("NCSC") to at least 'Foundation Grade', for example, under the 'NCSC Commercial Product Assurance' scheme ("CPA").

2.2 Devices used to access or manage Government Data and services must be under the management authority of *Client* or *Service Provider* and have a minimum set of security policy configuration enforced. These devices must be placed into a 'known good' state prior to being provisioned into the management authority of the *Client*. Unless otherwise agreed with the *Client* security representative in writing, all *Service Provider* devices are expected to meet the set of security requirements set out in the 'End User Devices Security Guidance' available at https://www.ncsc.gov.uk/guidance/end-user-device-security. Where the guidance highlights shortcomings in a particular platform the *Service Provider* may wish to use, then these should be discussed with the *Client* security representative and a joint decision shall be taken on whether the residual risks are acceptable. Where the *Service Provider* wishes to deviate from the NCSC guidance, then this should be agreed in writing on a case by case basis with the *Client* security representative.

3. Data Processing, Storage, Management and Destruction

3.1 The *Service Provider* and *Client* recognise the need for the *Client's* information to be safeguarded under the Data Protection Legislation. To that end, the *Service Provider* must be able to state to the *Client* security representative the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks Government Data will be subject to at all times.

3.2 The *Service Provider* shall agree any change in location of data storage, processing and administration with the *Client* security representative.

3.3 The *Service Provider* :

3.3.1 provides the *Client* security representative with all Government Data on demand in an agreed open format;

3.3.2 has documented processes to guarantee prompt availability of Government Data if the *Service Provider* stops trading;

3.3.3 securely destroys all Storage Media that has held Government Data at the end of life of that media using Good Industry Practice;

3.3.4 securely erases any or all Government Data held by the *Service Provider* when requested to do so by the *Client*; and

3.3.5 indemnifies the *Client* against any and all losses incurred if the *Service Provider* breaches this paragraph and any Data Protection Legislation.

4. Ensuring secure communications

4.1 The *Service Provider* shall ensure that any Government Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device is encrypted using a product or system component which has been formally assured through a certification process recognised by NCSC, to at least 'Foundation Grade', for example, under CPA.

4.2 The *Service Provider* shall use Good Industry Practice to maintain the configuration and use of all networking equipment to provide the *service*, including those that are located in secure physical locations.

5. Security by design

5.1 The *Service Provider* shall apply the 'principle of least privilege' (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of IT systems which will process or store Government Data.

5.2 When designing and configuring the ICT Environment (to the extent that the ICT Environment is within the control of the *Service Provider*) the *Service Provider* shall, using Good Industry Practice, seek guidance from recognised security professionals with the appropriate skills and/or a NCSC certification (https://www.ncsc.gov.uk/section/products-services/ncsc-certification) for all bespoke or complex components of the ICT Environment (to the extent that the ICT Environment is within the control of the *Service Provider*).

6. Security of Service Provider Staff

6.1 Service Provider Staff shall be subject to pre-employment checks that include, as a minimum: identity, unspent criminal convictions and right to work.

6.2 The *Service Provider* shall agree on a case by case basis Service Provider Staff roles which require specific government clearances (such as 'SC') including system administrators with privileged access to IT systems which store or process Government Data.

6.3 The *Service Provider* shall prevent Service Provider Staff who are unable to obtain the required security clearances from accessing systems which store, process, or are used to manage Government Data except where agreed with the *Client* security representative in writing.

6.4 All Service Provider Staff that have the ability to access Government Data or systems holding Government Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the *Client* security representative in writing, this training must be undertaken annually.

6.5 Where the *Service Provider* or Subcontractors grants increased ICT privileges or access rights to Service Provider Staff, those Service Provider Staff shall be granted only those permissions necessary for them to carry out their duties. When staff no longer need elevated privileges or leave the organisation, their access rights shall be revoked within one (1) Working Day.

7. Restricting and monitoring access

7.1 The *Service Provider* shall operate an access control regime to ensure all users and administrators of the ICT Environment (to the extent that the ICT Environment is within the control of the *Service Provider*) are uniquely identified and authenticated when accessing or administering the *service*. Applying the 'principle of least privilege', users and administrators shall be allowed access only to those parts of the ICT Environment that they require. The *Service Provider* shall retain an audit record of accesses.

8. Audit

8.1 The *Service Provider* shall collect audit records which relate to security events in the systems or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such *Service Provider* audit records should (as a minimum) include:

8.1.1 Logs to facilitate the identification of the specific asset which makes every outbound request external to the ICT Environment (to the extent that the ICT Environment is within the control of the *Service Provider*). To the extent the design of the *service* allows such logs shall include those from 'DHCP' servers, 'HTTP'/'HTTPS' proxy servers, firewalls and routers.

8.1.2 Security events generated in the ICT Environment (to the extent that the ICT Environment is within the control of the *Service Provider*) and shall include: privileged account log-on and log-off events, the start and termination of remote access sessions, security alerts from desktops and server operating systems and security alerts from third party security software.

8.2 The *Service Provider* and the *Client* security representative shall work together to establish any additional audit and monitoring requirements for the ICT Environment.

8.3 The *Service Provider* shall retain audit records collected in compliance with this paragraph 8 for a period of at least 6 months.

Annex 2 - Security Management Plan

REDACTED