SCHEDULE 18

Call-Off Schedule 9 (Security)

Part B: Long Form Security Requirements (Applicable to lots 1b, 1c, 2b, 2c,3b, 3c)

1. Definitions

1.1 In this Schedule the following words shall have the following meanings and they shall supplement Schedule 1 (Joint Schedule 1 - Definitions):

"Breach of Security"	means the occurrence of: a) any unauthorised access to or use of the *service*, the Sites 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);
"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; and
"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.

2. Security Requirements

2.1 The Client and the Service Provider recognise that, where specified in Framework Schedule 4 (Framework Management), CCS shall have the right to enforce the Client's rights under this Schedule.

2.2 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.

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

2.3.1 DEFRA Workplace FM24 Digital Workstream Lead;

2.3.2 Service Provider: [redacted].

2.4 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 and reviewed at least annually.

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

2.6 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.

2.7 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.

2.8 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, 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 during a Further Competition that it requires a bespoke ISMS, the ISMS provided by the Service Provider may be an extant ISMS covering the Services 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's Approval.

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 Premises, the Sites, the Supplier 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) where specified by a Client that has undertaken a Further Competition - 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) (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 (https://www.cpni.gov.uk), National Security Risk Assessment, National Risk register and National Resilience Standards.

g) complies with HMG Information Assurance Maturity Model and Assurance Framework (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 approvals 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 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 Representative of such inconsistency and the Client 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 pursuant to Paragraph 3.3.1 is Approved by the Client, it shall be adopted by the Service Provider immediately and thereafter operated and maintained in accordance with this Schedule. If the ISMS is not Approved by the Client, the Service Provider shall amend it within ten (10) Working Days of a notice of non-approval from the Client and re-submit it to the Client 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 fifteen (15) Working Days from the date of the first submission of the ISMS to the Client. If the Client does not Approve the ISMS following its resubmission, the matter shall be resolved in

accordance with the Dispute Resolution Procedure. No Approval to be given by the Client pursuant to this Paragraph 3 may be unreasonably withheld or delayed. However, any failure to approve the ISMS on the grounds that it does not comply with any of the requirements set out in Paragraphs 3.4 to 3.6 shall be deemed to be reasonable.

3.8 Approval by the Client 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 of reply* after the Contract Date, the *Service Provider* shall prepare and submit to the *Client* for Approval a Security Management Plan which shall comply with the requirements of this Schedule.

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);

4.2.2 comply with the 'Baseline Security Requirements' set out in Annex 1 to this Schedule and, where specified by the Client, in accordance with the Scope and Security Policies in Annex D – Policy, Documents and Standards;

4.2.3 identify the necessary delegated organisational roles defined for those responsible for ensuring the Scope 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 Affected Property, the Service Provider System, the Client System (to the extent 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* 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 Sites, 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 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 '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 Schedules and Scope 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* engaged in the *service* 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 *Service Manager*, 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 *Service Manager* will instruct the *Service Provider* to submit a revised Security Management Plan.

4.4 Approval by the *Service Manager* of the Security Management Plan shall not relieve the *Service Provider* of its obligations to deliver the *service*.

4.5 **Amendment of the ISMS and Security Management Plan**

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

4.6.1 emerging changes in Good Industry Practice;

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

4.6.3 any new perceived or changed security threats;

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

4.6.5 any new perceived or changed security threats; and

4.6.6 any reasonable change in requirement requested by the Client.

4.7 The Service Provider shall provide the Client 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:

4.7.1 suggested improvements to the effectiveness of the ISMS;

4.7.2 updates to the risk assessments;

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

4.7.4 suggested improvements in measuring the effectiveness of controls.

4.8 Subject to Paragraph 4.4, 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.

4.9 The Client may, acting reasonably, Approve and require changes or amendments to the ISMS or Security Management Plan to be implemented on timescales faster than set out in the Contract Data 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.

5. Security Testing

5.1 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. 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 in advance, the Service Provider shall be granted relief against any resultant under-performance for the period of the Security Tests.

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

5.3 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 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.

5.4 Where any Security Test carried out pursuant to Paragraphs 5.2 or 5.3 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 Approval, 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 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.

5.5 If any repeat Security Test carried out pursuant to Paragraph 5.4 reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall constitute a material Default of this Contract.

6. Complying with the ISMS

6.1 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).

6.2 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 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.

6.3 If, as a result of any such independent audit as described in Paragraph 6.1 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.

7. Security Breach

7.1 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.

7.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 7.1, the Service Provider shall:

7.2.1 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 Client Property and/or Client 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's ability to provide the *service* so as to meet the relevant KPI Performance Measures, 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 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.

7.3 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.

8. Vulnerabilities and fixing them

8.1 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.

8.2 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:

8.2.1 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

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

8.3 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 14 days of release, 'Important' within 30 days of release and all 'Other' within 60 Working Days of release, except where:

8.3.1 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*;

8.3.2 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 5 days, provided the Service Provider had followed and

continues to follow the security patch test plan agreed with the Client; or

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

8.4 The Specification and Mobilisation Plan (if applicable) shall include provisions for major version upgrades of all COTS Software to be upgraded within 6 Months of the release of the latest version, such that it is no more 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:

8.4.1 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

8.4.2 is agreed with the Client in writing.

8.5 The Service Provider shall:

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

8.5.2 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;

8.5.3 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;

8.5.4 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;

8.5.5 from the date specified in the Security Management Plan provide a report to the Client 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;

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

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

8.5.8 inform the Client 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.

8.6 If the Service Provider is unlikely to be able to mitigate the vulnerability within the timescales under this Paragraph 8, the Service Provider shall immediately notify the Client.

8.7 A failure to comply with Paragraph 8.3 shall constitute a Default, and the Service Provider shall comply with the Rectification Plan Process.

Part B – 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.

2. End user devices

2.1 When Government Data resides or is at rest 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, including those used by the Service Provider's subcontractors or subsubcontractors, 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 in writing, all Service Provider devices are expected to meet the set of security requirements set out in the 'End User Devices Security Guidance' (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 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.

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 UK Data Protection Legislation. To that end, the Service Provider must be able to state to the Client 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 Unless otherwise agreed by the *Client,* the Service Provider shall agree any change in location of data storage, processing and administration with the Client in accordance with Clause Z35.

3.3 The Service Provider shall:

3.3.1 provide the Client with all Government Data on demand in an agreed open format;

3.3.2 have documented processes to guarantee availability of Government Data in the event of the Service Provider ceasing to trade;

3.3.3 securely destroy all media that has held Government Data at the end of life of that media in line with Good Industry Practice; and

3.3.4 securely erase any or all Government Data held by the Service Provider when requested to do so by the Client.

4. Ensuring secure communications

4.1 The Client requires that any Government Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be 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 Client requires that the configuration and use of all networking equipment to provide the *service*, including those that are located in secure physical locations, are at least compliant with Good Industry Practice.

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 follow Good Industry Practice and 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 and during Mobilisation, which 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 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 in writing, this training must be undertaken annually.

6.5 Where the Service Provider or a Subcontractor grant increased ICT privileges or access rights to Service Provider Staff or Subcontractor 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 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 24 months.

Part B – Annex 2 - Security Management Plan

READ BEFORE EDITING: Convention used throughout this template:

1. Text in red italics is for guidance only and should be deleted prior to issue; and
2. Text in black has been provided as a guide and may be used directly in the final Plan.
3. 'Insert' is a Prompt Note that refers to 'action required'.
4. The completed Project Security Management Plan should be classified appropriately.

Project Security Management Plan

Insert Project Title here

Unique identifier Insert project number here

Doc No: Effective Date: *See note[1]*

Revision:

**Note 1 – Effective date. This needs to be in the future, a planned date after the signatures have been applied. This does two things: firstly, it makes a clear statement of when the document becomes the working point of reference for the project. Secondly, it gives the signatories a target date by which they must have signed up.*

Record of Revision of Project Security Management Plan

Revision No.	Revision Date	Brief Revision Description	Change Control
Insert Revision No. as applicable	Insert Revision date as applicable	Insert Revision Description, as applicable. Examples: • Issued for initial use • Issued due to added scope approved through	Change Control Number XXX, dated XXXXX

APPROVALS

Prepared by (Project/Organisation Security Officer):

Date:

Insert First and Surname
Insert author title

Approved by (Project/Activity Lead):

Date:

Insert First and Surname
Insert author title

Table of Contents

Use of This Template

The focus of this document is to describe and gain approval for the security management approaches and processes specific to this project. The Project Security Management Plan is initiated prior to contract acceptance, developed and reviewed continuously, and amended when there is a significant change to the project; such as change to the customer's requirement, transition of project phase and/or change to project management or funding.

This Template is intended to be tailored to fit the needs of each project. It provides guidance against a comprehensive list of sections to help plan and manage security and resilience effectively, to ensure secure delivery of the project itself, and to support the secure design of the products or services it delivers.

Purpose of the Project Security Management Plan

This Plan documents the supplier's security governance and management arrangements for the secure delivery of the project/activity. It also supports the development of the security case, which documents all information relating to the secure design of the products or services that the project delivers.
The Project Security Management Plan must document arrangements for how the project will:

- ***Comply** with the Authority's contractual security requirements and relevant security legislation/regulation and HM Government Standard 007: Security.*
- ***Manage** security risks that may impact time, cost or performance objectives, such as failure to achieve key milestones or acceptance criteria as a result of hostile action.*
- ***Control** the security of project activities and access to sensitive or critical assets by project stakeholders: assets, including information, people, equipment and infrastructure/sites.*
- ***Communicate** with customers, suppliers and other stakeholders about their security responsibilities, project security arrangements and security expectations.*
- ***Assure** stakeholders that security is well managed and security risks are within the risk appetites of risk owners.*

Project Definition

Scope

This section should define the intent of the project and establish a broad overview of:

- *Type of project, whether this is an equipment capability, support or service contract.*
- *Project priority, including how critical the capability will be to DEFRA (the Authority).*
- *Deliverable outputs, including products (platforms/systems) and services.*

- *Project work breakdown, including activities undertaken by DEFRA, sub-contractors, or academia.*

Asset Categorisation and Policy, Legal and Regulatory Requirements

The project is to define any applicable legislation, regulatory requirements that the project will need to adhere to. This section must also demonstrate how the project shall achieve compliance with security Legislation and/or Regulation.

Governance

The Project must identify the supplier's Senior Responsible Owner (SRO) who owns the project's security risks. A Project/Activity Lead should also be identified who can be accountable to the project SRO for the management of Project security risks. The table below provides an indicated list of roles that should be identified. This is not an exhaustive list and should be added to as necessary:

Role	**Name of individual/representative**
Project Sponsor/SRO	*Owns the capability and holds the overall responsibility, accountability and authority for all associated risks*
Project Team Leader	*Accountable to the SRO for the management of project security risk; secure delivery and secure design.*
Project Manager	*Responsible for the delivery of good project security outcomes*
Project/Organisation Security Officer (PSyO)	*Responsible for the co-ordination of project security activities and an advisor to project stakeholders on matters of security management and the associated project risks*
Security Architect	*Responsible for the co-ordination of security architecture activities and an advisor to project stakeholders on matters of cyber resilience and associated risks*

Security Working Group

A Security Working Group or alternative suitable forum for the discussion of security activities, risks and issues should be available within the Project team. This section should detail the role of the Security Working Group or alternative forum and its accountabilities.

Responsibility Assignment

A Project Security Assignment RACI Matrix, together with the Security Working Group Terms of Reference, is recommend and should define responsibilities for:

- *Compliance with regulatory or assurance processes*.
- *Identification of project security risks and issues and escalation, as necessary.*
- *Out of scope reporting.*
- *Communication of security awareness requirements, including qualifications/training.*
- *Management of security links with other projects, establishments or external support contracts, including dependencies on business continuity and disaster recovery.*
- *Definition of project/contract asset disposal plans*

Security Management

The project must define the processes used to identify, assess and manage security risks to people, process, technology or infrastructure.

Methodology

Define how security risks are managed, please highlight any specific corporate processes used and where the risks will be recorded. Please also highlight any specific guidance to be used for the identification and assessment of security risks and how oversight will be achieved.

Project Risk Reviews *shall review and prioritise the risks to secure delivery, recorded in the Project risk register. The Project shall ensure sufficient visibility of current risk assessments for discussion, response planning and management.*

As a minimum, the project should maintain the following Security Management artefacts:

- *Business Impact Analysis (BIA): Identifies dependencies and the impact of disruption to understand criticality.*
- *Threat Assessment: Identifies threat actors who would seek to compromise or disrupt the project or attack the in-service capability, and assesses their doctrine and likely capability to mount attacks.*
- *Asset Register: a register of all sensitive and critical assets that are under the control of project stakeholders, including industry partners.*
- *Security Risk Records: Entries within the project risk register.*
- *Implementation plans for asset controls and security measures*

Business Impact Analysis

The project BIA should cover the project's dependencies to deliver the service or activity, however the project should also support the customer to develop their BIA for the in-service capability, which should inform the project's requirement for its support solution design.

The project must also identify any critical dependencies: Examples only (not exhaustive);

- *Specialist personnel, including Project staff, contractors and Industry staff.*
- *Infrastructure and utilities, such as DEFRA establishments, including project headquarters or Industry Facilities.*
- *Information management systems, whether DEFRA or third-party.*
- *Dependencies upon external service providers; other projects, establishments, facilities.*
- *Critical supply chains.*

Threat Assessment

This section should be considered carefully for classification. Threat assessments may need to be held at higher classification than the rest of the Plan.

The project Threat Assessment is a process to determine the credibility and seriousness of a potential threat as well as the probability that the threat will become a reality, by categorising the nature of the threat actors, and their capabilities, that pose a risk to the project and its outputs. Threat assessments should be developed to inform the SRO and End Users of the risks to the project and in-service capability.

Threat Assessments can be developed by drawing from or collaborating with:

- *UK National Cyber Secruity Centre (NCSC) (www)*

- *US National Institute of Standards and Technology (NIST) (Information Security Special Publication 800-30: Guide for Conducting Risk Asessments; Appendix D, Threat Sources)*
- *Centre for the Protection of National Infrastructure (www)*
- *Industry Partners*

The project must identify the primary sources of threat supported by a detailed Threat Assessments appended to this Plan.

Asset Register

DEFRA considers an asset to be any useful or valuable item, the compromise of which would cause either disruption or loss of a capability. Assets are to some degree sensitive, critical or both. Sensitive assets are typically identifiable by their classification and critical assets are those upon which we are most dependent, identifiable from the BIA; critical assets are those with a high consequence of failure, irrespective of whether failure is likely or not. Sensitive and critical assets require safeguarding through compliance with the Security Aspects Letter. Such assets include:

- *Equipment, including platforms, systems, office equipment and furniture;*
- *Resources, such as people and finances;*
- *Infrastructure, such as establishments, buildings and utilities infrastructure;*
- *Information, held electronically or on paper, relating to subjects such as policy, process and procedure, projects, research and development, products and services, intellectual property, training, commercial, decision making, financial, legal, and compliance, communications and business operations, logistics and support.*

All project assets are to be recorded in an Asset Register and appended to this Plan, which details the following:

- *Asset type, such as Platform, System or Equipment.*
- *Asset description; a brief overview.*
- *Asset owner; responsible for asset management and accountable to risk owner.*
- *Asset Classification; OFFICIAL, SECRET or TOP SECRET, including codewords*
- *Asset utility/impact grading, using Impact Levels or other scale.*
- *Essential services to maintain or use the asset.*

Security Risk Records

Risks to the confidentiality, integrity or availability of project assets that may impact the secure delivery of the project or its outputs are identified and assessed. The BIA and identification of Critical Assets drives the priorities for risk control and mitigation, which are reviewed and agreed by the Project/Activity Lead. All risks shall be acceptable to the SRO.

Asset Controls

The Implementation of asset controls is the responsibility of the asset owners, who are accountable to the relevant risk owners for secure handling of assets. The Project must ensure that asset controls are communicated through appropriate tools:

- *Security risk records*
- *Technical documentation, such as operating procedures*
- *Additional governance processes documented within the governance section*

Grading Guide

It is the responsibility of the Project/Activity Lead to ensure that the management of Authority/Client assets is managed in accordance with the Security Aspects Letter and SCAH Programme Grading Guide.

The 'SCAH Programme Grading Guide' ensures that the classification of all assets involved throughout the life of the project is clearly defined. The guide also includes the mechanisms for requesting changes to classifications, disposal and destruction, and considers how assets will be classified if international partners are involved. The 'Grading Guide' is appended to this Plan at Annex G.

Security Arrangements and Measures

Business Continuity & Incident Management

The Project/Activity must have a Business Continuity Plan (BCP), ideally developed in line with ISO 22301. The project must identify its critical outputs or capability and ensures that Subcontractors and industry suppliers have Business Continuity measures in place to mitigate disruptions. The Service Provider's BCP's should be appended to this Plan.

The Plan must indicate the actions the Service Provider will take in the event of an incident to continue delivering essential tasks, activities and services throughout the recovery process. The Plan shall also include a response structure that will enable timely warning and communication to the Authority.

Personnel Security

A system of policies and procedures which aim to manage and minimise the risks of human error, loss, theft, fraud or misuse of Authority assets. The Project must establish governance processes, appended to the Plan to ensure that:

- *Vetting requirements, with any nationality restrictions, are well defined according to need to know, need to hold and need to access information and/or locations.*
- *Where necessary, international collaboration is well managed.*

- *Contracts with third party suppliers have appropriate clauses covering personnel security, access control and disclosure/confidentiality management.*
- *Security expectations are established and communicated across all project stakeholders, for:*
    - *Culture and awareness activities, including training.*
    - *Safety & Security briefings and inductions.*
    - *Personal responsibilities for policy compliance and good security behaviors.*
    - *Access control requirements for Buyer Premises.*

Physical Security

Physical security is the protection of people, property and physical assets from actions and events that could cause damage or loss. The project should prioritise physical security against forcible and surreptitious attack that may compromise assets in the following way:

- *People or infrastructure – priority protection from harm/damage. People are adequately protected from the risk of terrorist attack and infrastructure is protected from sabotage commensurate with the threat and operational criticality.*
- *Information or equipment – priority protection from theft, damage or undetected compromise. Surreptitious protections are commensurate with classification*

  (Confidentiality requirements) and forcible protections are commensurate with operational criticality (integrity and availability requirements).

The Plan must indicate how the Project shall manage physical security against the requirements of the Security Aspects Letter. Where risks are identified, either by non-compliance or through the project's Security Management regime, these are recorded in the Project risk register and escalated to the Authority accordingly.

Information Security

The project should recognise that information security is the practice of preventing unauthorised access, use, disclosure, disruption, modification, inspection, recording or destruction of information and is a critical asset and needs to be assured, protected and shared securely.

In accordance with Government requirements, all suppliers bidding for project contracts involving the handling of sensitive or personal information will be required to protect these assets to standards laid down. They will be certified against the 'Cyber Essentials scheme'.

The Plan must indicate how the Project shall manage information security against the requirements of the Security Aspects Letter. Where risks are identified, either by

non-compliance or through the project's Security Management regime, these are recorded in the Project risk register and escalated to the Authority accordingly.

Advisory Annexes

A. **Glossary**

B. **Policy, Legislation and Regulation**

C. **Terms of Reference and Responsibility Assignments**

D. **Business Impact Analysis**

E. **Threat Assessment**

F. **Registers of Assets and Risks**

G. **Grading Guide**

H. **Supplier Business Continuity Plans**