HM Revenue & Customs

HMRC Tier 3 Model ICT Contract
Version 2.0 (April 2019)

SCHEDULE 2.4 | Security Management

Schedule 2.4 | Security Management

1 DEFINITIONS

In this Schedule, the following definitions shall apply:

"Breach of Security"	the occurrence of: (a) any unauthorised access to or use of the Services, the Authority Premises, the Sites, the Supplier System, the Authority System (to the extent that it is under the control of the Supplier) and/or any IT, information or data (including the Confidential Information and the Authority Data) used by the Authority and/or the Supplier in connection with this Agreement; and/or (b) the loss, corruption and/or unauthorised disclosure of any information or data (including the Confidential Information and the Authority Data), including any copies of such information or data, used by the Authority and/or the Supplier in connection with this Agreement; and/or (c) a failure to comply with the personnel security requirements, as set out in the Security Management Plan, in either case as more particularly set out in the Security requirements in Schedule 2.1 (Services Description) and the Baseline Security Requirements;
"CCP"	CESG Certified Practitioner;
"CESG"	the UK Government's national technical authority for information assurance;
"CHECK Scheme"	The scheme for penetration testing of data processing systems operated by the CESG;
"CPA"	the CESG Commercial Product Assurance scheme;
"CPNI"	Centre for Protection of National Infrastructure;
"ISMS"	the information security management system and processes developed by the Supplier in accordance

	with Paragraph 3 as updated from time to time in accordance with this Schedule;
"Security Policy Framework"	the Security Policy Framework published by the Cabinet Office as updated from time to time including any details notified by the Authority to the Supplier;
"Security Management Plan"	is the document produced by the Supplier, a copy of which is at Annex 2;
"Security Questionnaire"	the questionnaire produced by the Authority which, when completed by the Supplier, will form the basis of the Supplier's Security Management Plan; and
"Security Tests"	tests carried out where relevant in accordance with the CHECK Scheme or to an equivalent standard to validate the ISMS and security of all relevant processes, systems, incident response plans, patches to vulnerabilities and mitigations to Breaches of Security.

2 INTRODUCTION

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 Agreement will be met.

2.2 The Authority shall clearly articulate its high level security requirements so that the Supplier can ensure that the ISMS, security related activities and any mitigations are driven by these fundamental needs.

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

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

2.5 The Supplier shall ensure the up-to-date maintenance of a security policy relating to the operation of its own buildings, organisation and systems and on request shall supply this document as soon as practicable to the Authority.

2.6 The Supplier's own security policy should, align with the contents of the Security Management Plan and incorporate CESG and CPNI best practice.

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

2.8 NOT USED

2.9 The Supplier must adhere to the physical, people and technical security controls for Off-Shore Locations which have been agreed with the Authority.

3 ISMS

3.1 Within twenty-one (21) days of the Effective Date, the Supplier shall develop and submit to the Authority for the Authority's approval in accordance with Paragraph 3.6 an ISMS (information security management system) for the purposes of this Agreement, which:

(a) shall have been tested in accordance with Schedule 6.2 (*Test and Assurance*); and

(b) shall comply with the requirements of Paragraphs 3.3 to 3.5.

3.2 The Supplier acknowledges that the Authority places great emphasis on the reliability of the Services and confidentiality, integrity and availability of information and consequently on the security provided by the ISMS and agrees that it shall be responsible for the effective performance of the ISMS.

3.3 The ISMS shall:

(a) unless otherwise specified by the Authority in writing, be developed to protect all aspects of the Services and all processes associated with the delivery of the Services, including the Authority Premises, the Sites, the Supplier System, the Authority System (to the extent that it is under the control of the Supplier) and any IT, information and data (including the Authority Confidential Information and the Authority Data) to the extent used by the Authority or the Supplier in connection with this Agreement;

(b) meet the relevant requirements in ISO/IEC 27001 and ISO/IEC 27002 in accordance with Paragraph 7; and

(c) at all times provide a level of security which:

(i) is in accordance with Law and this Agreement;

(ii) as a minimum demonstrates Good Industry Practice;

(iii) complies with the Baseline Security Requirements;

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

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

(vi) complies with the security requirements as set out in Schedule 2.1 (*Services Description*);

(vii) complies with the Authority's IT policies; and

(viii) is in accordance with the Security Policy Framework;

(d) document the security incident management processes and incident response plans;

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

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

3.4 Subject to Clause 20 (*Authority Data and Security Requirements*) the references to standards, guidance and policies set out in Paragraph 3.3 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.

3.5 In the event that the Supplier becomes aware of any inconsistency in the provisions of the standards, guidance and policies set out in Paragraph 3.3, the Supplier shall immediately notify the Authority Representative of such inconsistency and the Authority Representative shall, as soon as practicable, notify the Supplier which provision the Supplier shall comply with.

3.6 If the ISMS submitted to the Authority pursuant to Paragraph 3.1 is approved by the Authority, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the ISMS is not approved by the Authority, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Authority and re-submit it to the Authority for approval. The Parties shall use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Authority. If the Authority does not approve the ISMS following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Authority pursuant to this Paragraph 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 3.3 to 3.5 shall be deemed to be reasonable.

3.7 Approval by the Authority of the ISMS pursuant to Paragraph 3.6 or of any change to the ISMS shall not relieve the Supplier of its obligations under this Schedule.

4 SECURITY MANAGEMENT PLAN

4.1 Within twenty (20) Working Days after the Effective Date, the Supplier shall prepare and submit to the Authority for approval in accordance with Paragraph 4.3 a 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:

(a) be based on the Supplier's final response to the Authority's Security Questionnaire;

(b) comply with the Baseline Security Requirements set out in Annex 1;

(c) identify the necessary delegated organisational roles defined for those responsible for ensuring this Schedule is complied with by the Supplier;

(d) detail the process for vetting staff at the appropriate security level with reference to the level of access staff will have to Authority Data, managing any security risks from Sub-contractors and third parties authorised by the Authority with access to the Services, processes associated with the delivery of the Services, the Authority Premises, the Sites, the Supplier System, the Authority System (to extent that it is under the control of the Supplier) and any IT, Information and data (including the Authority Confidential Information and the Authority Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Services;

(e) unless otherwise specified by the Authority in writing, be developed to protect all aspects of the Services and all processes associated with the delivery of the Services, including the Authority Premises, the Sites, the Supplier System, the Authority System (to the extent that it is under the control of the Supplier) and any IT, Information and data (including the Authority Confidential Information and the Authority Data) to the extent used by the Authority or the Supplier in connection with this Agreement or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Services;

(f) set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Services and all processes associated with the delivery of the Services and at all times comply with and specify security measures and procedures which are sufficient to ensure that the Services comply with the provisions of this Schedule (including the requirements set out in Paragraph 3.4);

(g) demonstrate that the Supplier Solution has minimised the Authority and Supplier effort required to comply with this Schedule through consideration of available, appropriate and practicable pan-government accredited services (for example, 'platform as a service' offerings from the G-Cloud catalogue);

(h) set out the plans for transiting all security arrangements and responsibilities from those in place at the Effective Date to those incorporated in the ISMS at the date set out in Schedule 6.1 (*Implementation*) for the Supplier to meet the full obligations of the security requirements set out in Schedule 2.1 (*Services Description*) and this Schedule;

(i) set out the scope of the Authority System that is under the control of the Supplier;

(j) be structured in accordance with ISO/IEC 27001 and ISO/IEC 27002, cross-referencing if necessary to other Schedules which cover specific areas included within those standards;

(k) be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Authority engaged in the Services and shall reference only documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule; and

(l) be in accordance with the Security Policy Framework.

4.3 If the Security Management Plan submitted to the Authority Representative pursuant to Paragraph 4.1 is approved by the Authority Representative, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not approved by the Authority Representative, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Authority and re-submit it to the Authority Representative 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 (or such other period as the Parties may agree in writing) from the date of its first submission to the Authority Representative. If the Authority Representative does not approve the Security Management Plan following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Authority Representative pursuant to this Paragraph 4.3 may be unreasonably withheld or delayed. However any failure to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.

4.4 Approval by the Authority of the Security Management Plan pursuant to Paragraph 4.3 or of any change or amendment to the Security Management Plan shall not relieve the Supplier of its obligations under this Schedule.

5 AMENDMENT AND REVISION OF THE ISMS AND SECURITY MANAGEMENT PLAN

5.1 The ISMS and Security Management Plan shall be fully reviewed and updated by the Supplier within ten (10) Working Days of any Breach of Security and further at least annually to reflect:

(a) emerging changes in Good Industry Practice;

(b) any change or proposed change to the IT Environment, the Services and/or associated processes;

(c) any new perceived or changed security threats; and

(d) any reasonable change in requirements requested by the Authority.

5.2 The Supplier shall provide the Authority 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 Authority. The results of the review shall include, without limitation:

(a) suggested improvements to the effectiveness of the ISMS;

(b) updates to the risk assessments;

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

(d) suggested improvements in measuring the effectiveness of controls.

5.3 Subject to Paragraph 5.4, any change which the Supplier proposes to make to the ISMS or Security Management Plan (as a result of a review carried out pursuant to Paragraph 5.1, an Authority request, a change to Schedule 2.1 (*Services Description*) or otherwise) shall be subject to the Change Control Procedure and shall not be implemented until approved in writing by the Authority.

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

6 SECURITY TESTING

6.1 The Supplier shall conduct relevant Security Tests from time to time (and at least annually across the scope of the ISMS) and additionally after significant architectural changes to the IT Environment or after any change or amendment to the ISMS, (including security incident management processes and incident response plans) or the Security Management Plan. Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Authority. The Supplier shall conduct, document and provide to the Authority a risk assessment to enable the Authority to consider whether a Security Test should be carried out. Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier's ability to deliver the Services so as to meet the Target Performance Levels, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests.

6.2 The Authority shall be entitled to send a representative to witness the conduct of the Security Tests. The Supplier shall provide the Authority with the results of such tests (in a form approved by the Authority 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 Authority pursuant to this Agreement, the Authority and/or its authorised representatives shall be entitled, at any time upon giving reasonable notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the Supplier's compliance with the ISMS and the Security Management Plan. The Authority may notify the Supplier of the results of such tests after completion of each such test. If any such Authority test adversely affects the Supplier's ability to deliver the Services so as to meet the Target Performance Levels, the Supplier shall be granted relief against any resultant under-performance for the period of the Authority 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 Supplier shall promptly notify the Authority of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Authority's prior written approval, the Supplier shall implement such changes to the ISMS and the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Authority 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 Baseline Security Requirements or security requirements (as set out in Schedule 2.1 (*Services Description*)) or the requirements of this Schedule, the change to the ISMS or Security Management Plan shall be at no cost to the Authority.

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, such circumstance shall constitute a material Default for the purposes of Clause 27 (*Rectification Plan Process*).

7 ISMS COMPLIANCE

7.1 The Authority 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, the specific security requirements set out in Schedule 2.1 (*Services Description*) and the Baseline Security Requirements.

7.2 If, on the basis of evidence provided by such audits, it is the Authority's reasonable opinion that compliance with the principles and practices of ISO/IEC 27001, the specific security requirements set out in Schedule 2.1 (*Services Description*) and/or the Baseline Security Requirements is not being achieved by the Supplier, then the Authority shall notify the Supplier of the same and give the Supplier a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to implement any necessary remedy. If the Supplier does not become compliant within the required time then the Authority shall have the right to obtain an independent audit against these standards in whole or in part. The Supplier shall reimburse in full the costs incurred by the Authority in obtaining such audit.

7.3 If, as a result of any such independent audit as described in Paragraph 7.2 the Supplier is found to be non-compliant with the principles and practices of ISO/IEC 27001, the specific security requirements set out in Schedule 2.1 (*Services Description*) and/or the Baseline Security Requirements then the Supplier shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and, (as said above), shall reimburse in full the costs incurred by the Authority in obtaining such audit.

8 BREACH OF SECURITY

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

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 Supplier shall:

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

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

(ii) remedy such Breach of Security to the extent possible and protect the integrity of the IT Environment to the extent within its control against any such Breach of Security or attempted Breach of Security;

(iii) 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 Supplier, if the mitigation adversely affects the Supplier's ability to deliver the Services so as to meet the Target Performance Levels, the Supplier shall be granted relief against any resultant under-performance for such period as the Authority, acting reasonably, may specify by written notice to the Supplier;

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

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

(b) as soon as reasonably practicable provide to the Authority 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 Authority.

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 Baseline Security Requirements or security requirements (as set out in Schedule 2.1 (*Services Description*)) or the requirements of this Schedule, then any required change to the ISMS shall be at no cost to the Authority.

9 VULNERABILITES AND CORRECTIVE ACTION

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

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

(a) 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

(b) Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two (2) remaining levels ('Moderate' and 'Low') respectively.

9.3 The Supplier shall procure the application of security patches to vulnerabilities (whether such patches are entirely related to security or related in part to security) within a maximum period from the public release of such patches with those vulnerabilities categorised as 'Critical' within fourteen (14) days of release, 'Important' within thirty (30) days of release and all 'Other' within sixty (60) Working Days of release, except where:

(a) the Supplier 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 Supplier asserts cannot be exploited within the context of a Service must be remedied by the Supplier within the above timescales if the vulnerability becomes exploitable within the context of the Service;

(b) the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of 5 days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Authority; or

(c) the Authority agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the ISMS.

9.4 The Supplier Solution and Implementation Plan shall include provisions for major version upgrades of all Supplier Software and Third Party Software to be upgraded within six (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 Term unless:

(a) where upgrading such Supplier Software and Third Party Software reduces the level of mitigations for known threats, vulnerabilities or exploitation techniques, provided always that such upgrade is made within twelve (12) months of release of the latest version; or

(b) is agreed with the Authority in writing.

9.5 The Supplier shall:

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

(b) ensure that the IT Environment (to the extent that the IT Environment is within the control of the Supplier) is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

(c) ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the IT Environment by actively monitoring the threat landscape during the Term;

(d) pro-actively scan the IT Environment (to the extent that the IT Environment is within the control of the Supplier) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS as developed under Paragraph 3.3(e);

(e) from the date specified in the Security Management Plan (and before the first Operational Service Commencement Date) provide a report to the Authority within five (5) Working Days of the end of each month detailing both patched and outstanding vulnerabilities in the IT Environment (to the extent that the IT Environment is within the control of the Supplier) and any elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report;

(f) propose interim mitigation measures to vulnerabilities in the IT Environment known to be exploitable where a security patch is not immediately available;

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

(h) inform the Authority when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the IT Environment and provide initial indications of possible mitigations.

9.6 If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under Paragraph 9, the Supplier shall immediately notify the Authority.

9.7 A failure to comply with Paragraph 9.3 shall constitute a Notifiable Default, and the Supplier shall comply with the Rectification Plan Process.

ANNEX 1 | Baseline Security Requirements

1 Higher Classifications

1.1 The Supplier shall not handle Authority Materials classified SECRET or TOP SECRET except if there is a specific requirement and in this case prior to receipt of such information the Supplier shall seek additional specific guidance from the Authority.

2 End User Devices

2.1 When Authority 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 CESG to at least Foundation Grade, for example, under CPA.

2.2 Devices used to access or manage Authority Data and services must be under the management authority of Authority or Supplier 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 Authority. Unless otherwise agreed with the Authority in writing, all Supplier devices are expected to meet the set of security requirements set out in the CESG End User Devices Platform Security Guidance (https://www.gov.uk/government/collections/end-user-devices-security-guidance--2). As a minimum, the security standards must include Assurance Framework, Ten Critical Steps and Requirements. Where the guidance highlights shortcomings in a particular platform the Supplier may wish to use, then these should be discussed with the Authority and a joint decision shall be taken on whether the residual risks are acceptable. Where the Supplier wishes to deviate from the CESG guidance, then this should be agreed in writing on a case by case basis with the Authority.

3 Data Processing, Storage, Management and Destruction

3.1 The Supplier and Authority recognise the need for the Authority Data to be safeguarded under the UK Data Protection regime or a similar regime. To that end, the Supplier must be able to state to the Authority the physical locations in which Authority Data may be stored, processed and managed from, and what legal and regulatory frameworks Authority information will be subject to at all times.

3.2 The Supplier shall agree any change in location of Authority Data storage, processing and administration with the Authority in advance where the proposed location is outside the UK. The Authority's agreement to any such change shall be entirely at the Authority's discretion and, in so far as the change in location entails the move of Personal Data to an Off-shore Location, shall only be given if a Change Request is expressly permitted by Clause 23.8 (*Protection of Personal Data*), and such agreement shall in all circumstances be dependent upon the storage, processing and management of any Authority Data being carried out offshore within:

(a) the European Economic Area (EEA);

(b) the US if the Supplier and or any relevant Sub-contractor have signed up to an agreement which ensures a level of protection which has been defined as adequate by the EU Commission; or

(c) another country or territory outside the EEA if that country or territory ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into which have been defined as adequate by the EU Commission and approval has been provided by the Authority's Digital Information Officer or Office of Government Serious Information Risk Officer.

3.3 The Supplier shall:

(a) provide the Authority with all Authority Data on demand in an agreed open format;

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

(c) securely destroy all media that has held Authority Data at the end of life of that media in line with Good Industry Practice; and

(d) securely erase any or all Authority Data held by the Supplier when requested to do so by the Authority.

4 Networking

4.1 The Authority requires that any Authority 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 CESG, to at least Foundation Grade, for example, under CPA or through the use of pan-government accredited encrypted networking services via the Public Sector Network ("PSN") framework (which makes use of Foundation Grade certified products).

4.2 The Authority requires that the configuration and use of all networking equipment to provide the Services, including those that are located in secure physical locations, are at least compliant with Good Industry Practice.

5 Security Architectures

5.1 The Supplier 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 Authority Materials.

5.2 When designing and configuring the IT Environment (to the extent that the IT Environment is within the control of the Supplier) the Supplier shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or a CESG Certified Professional certification (http://www.cesg.gov.uk/awarenesstraining/IA-certification/Pages/index.aspx) for all bespoke or complex components of the Supplier Solution.

6 Personnel Security

6.1 Supplier Personnel shall be subject to pre-employment checks that include, as a minimum: identity, unspent criminal convictions and right to work (including nationality and immigration status).

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

6.3 The Supplier shall prevent Supplier Personnel who are unable to obtain the required security clearances from accessing systems which store, process, or are used to manage Authority Data except where agreed with the Authority in writing.

6.4 All Supplier Personnel that have the ability to access Authority Data or systems holding Authority Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Authority in writing, this training must be undertaken annually.

6.5 Where the Supplier or Sub-Contractors grants increased IT privileges or access rights to Supplier Personnel, those Supplier Personnel 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 1 Working Day.

6.6 Notwithstanding the Supplier's obligation to ensure that the Security Management Plan is implemented and followed, the Supplier shall ensure that the Supplier Personnel are promptly informed of action taken in relation to any failure to do so.

6.7 The Supplier shall ensure that Supplier Personnel complete the security questionnaire as provided by the Authority from time to time.

6.8 The Supplier shall perform the Off-Shore Personnel Security Checks in relation to any proposed Off-Shore Personnel prior to their engagement to the reasonable satisfaction of the Authority in the delivery of the Services under this Agreement.

7 Identity, Authentication and Access Control

7.1 The Supplier shall operate an access control regime to ensure all users and administrators of the Supplier Solution are uniquely identified and authenticated when accessing or administering the Services. Applying the 'principle of least privilege', users and administrators shall be allowed access only to those parts of the Supplier Solution they require. The Supplier shall retain an audit record of accesses.

8 Audit and Monitoring

8.1 The Supplier 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 Supplier audit records should (as a minimum) include:

(a) Logs to facilitate the identification of the specific asset which makes every outbound request external to the IT Environment (to the extent that the IT Environment is within the control of the Supplier). To the extent the design of the Supplier Solution and Services allows such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers.

(b) Security events generated in the IT Environment (to the extent that the IT Environment is within the control of the Supplier) and shall include: privileged account logon and logoff 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 Supplier and the Authority shall work together to establish any additional audit and monitoring requirements for the IT Environment.

8.3 The Supplier shall retain audit records collected in compliance with Paragraph 7.1 for a period of at least six (6) months.

1.Security Principles

•	1.1 The HMRC policy is that no HMRC data should be stored, accessed, processed, backed up or viewed outside the UK without prior approval. If you will be offshoring for this contract, we will ask you to consider using UK based processes instead. If this is not possible, you will need to go through HMRC's internal approval process, providing details of your organisational and technical measures to safeguard HMRC data. Please note approval is not guaranteed. *Please note: In line with HMRC's policies in response to current regulatory guidance, the successful supplier(s) will not be permitted to transfer any Personal Data (as defined in the General Data Protection Regulation (GDPR)) provided by HMRC in connection with any contract resulting from this procurement exercise, to the United States of America.* *On this basis, HMRC reserves the right to reject a bidder's entire tender submission and/or terminate any contract awarded, where it becomes apparent to HMRC that the supplier is transferring/is proposing to transfer Personal Data to the United States of America.*
•	1.2 Where the term HMRC asset is used in this questionnaire this includes paper and electronic HMRC data (e.g. customer, staff, location), as well as physical assets e.g. furniture and IT equipment.
•	1.3 The term sub-contractor applies to any third party who will be employed in delivering part of the service for HMRC such as suppliers, including IT providers, disposal agents, freelancers, self-employed staff etc... All requirements listed will apply to those in the supply chain who will deliver the service.
•	1.4 Third party suppliers of Cloud Services, whether Infrastructure as a Service (IAAS), Platform as a Service (PAAS) or Software as a Service (SAAS) must follow the National Cyber Security Centre (NCSC) 14 principles
•	1.5 When dealing with HMRC personal data the General Data Protection Regulation (GDPR) requirements are followed
•	1.6 When dealing with HMRC personal data the Data Protection Act 2018 (DPA 2018) requirements are followed

2. Mandatory Security Requirements

Please confirm:

• 2.1 That you understand that your responses to this questionnaire will form the initial Security Plan and will be included in the final signed version of any resulting agreement.	REDACTED
• 2.2 That you understand and agree that the transfer of HMRC assets and data outside the supply chain is prohibited without prior written consent from HMRC. If you do intend to share HMRC data with any party outside of the named supply chain other than for delivery of this contract, please inform HMRC.	REDACTED
• 2.3 That you understand that HMRC's policy is that no HMRC or customer data should be stored, processed, accessed, backed-up or viewed outside the UK without prior approval. If you do intend to do this, please note that there will be an additional application process to follow, and approval is not guaranteed.	REDACTED
• 2.4 Your Data Protection registration number. More information can be found at Data Protection Register	REDACTED
• 2.5 That in the event that your bid is successful, all contractor's personnel who have access to HMRC data and/or assets will provide signed hard copies (or electronic) of HMRC's Confidentiality Agreement (CA) if requested.	REDACTED

• 2.6 Access to HMRC assets is limited to only those who need it.	We confirm this

OFFICIAL

Physical Requirements	
High Level Requirements	**Supporting Requirements**
• You must have a process in place to control access to your premises and HMRC assets	• Buildings to be constructed of robust materials, typically brick or lightweight block walls • External access points to the building to be kept to a minimum, but in line with Health & Safety and Fire Regulations • All potential entry points to the building and assets to be secured out of hours • A process in place to control access to keys and codes that enable entry to the premises • A process in place to manage visitors • Secret (or above) List X certification or evidence an application is in progress • HMRC assets to be stored in appropriate security furniture/rooms out of hours • Installation of an Intruder Detection System with key holder response out of hours is required, as is a strong recommendation for external CCTV & lighting • Employ 24/7 security personnel

Please provide details of the premises from which this service/contract will be operated from (include separately any other locations such as warehouses and sub-contractor premises). Detail measures such as: -

- Procedures covering end of day/silent hours
- Key management
- Visitor controls
- Automated access controls
- Alarms
- Perimeter Security
- Guard patrols
- CCTV coverage
- Maintenance schedule of these security controls

REDACTED
Will you be handling at least 'Secret' HMRC information in delivering this contract? (if not please do not answer this question) - If 'yes', please provide the following: ● Your List X certification ● What is the name of your Security Controller? ● What/Where does the List X accreditation cover? ● For what purpose? ● Evidence that the Department who sponsored the List X accreditation has agreed to share the environment.
REDACTED

Personnel Requirements	
High Level Requirements	**Supporting Requirements**
● All personnel and sub-contractors dealing with HMRC assets/data to have the appropriate formal NSV security clearance, with Baseline Personnel Security Standards	● There will be accountable owner(s) for personnel risk within the organisation ● There will be established, and communicated senior commitment to a strong security culture, consistent at all levels of the organisation ● There will be a process for risk assessing all roles within an organisation to identify most appropriate personnel security controls ● There will be additional processes for screening for higher risk roles where appropriate (formal NSV security clearance)

(BPSS) as a minimum	
• You must have a security governance framework which coordinates and directs its management of the service and information within it	• There will be induction and ongoing training in security awareness for all staff and sub-contractors working on the HMRC contract • There will be established and defined joining and leaving procedures for staff • There will be disciplinary process for staff where there has been a security breach • Clear articulation of expectations of staff in a range of areas having clear published policies on acceptable use of information etc • Policies for monitoring staff for 'insider threats'

How do you ensure that any staff who will have access to, or come in to contact with, HMRC data or assets have undergone BPSS checks or equivalent (this also applies to your supply chain for the delivery of this service). What are your procedures for assessing roles for more enhanced vetting and applying for these?
REDACTED
What are your procedures for recruitment of staff, giving them systems access and set up. Please outline how you amend system accesses with a change of role. What are your processes termination of employment including how you manage retrieval of data and/or assets and revoking access to your systems and premises.
REDACTED
How will you ensure that all staff accessing HMRC data are aware of the confidential nature of the data and comply with their legal and specific obligations under the Contract?

REDACTED
What security training is in place for employees prior to accessing HMRC data or assets - how this training is carried out initially, and on an ongoing basis including testing of understanding. Are there different levels of training depending on the job function within the organisation?
REDACTED
How are all staff made aware of the organisations' security policy and potential sanctions for inappropriate behaviour?
REDACTED

Cyber Requirements	
High Level Requirements	**Supporting Requirements**
• All suppliers bidding for government contracts will have achieved at least Cyber Essentials or Cyber Essentials+	• The supplier must demonstrate a minimum level of cyber security controls to safeguard HMRC data and assets
• Users must be given the minimum access to sensitive information or key operational services	• Processes are in place to manage the authentication, authorisation and privileges of users and privileged users, including a Joiners/Movers/Leavers process • Processes for the patching, secure configuration and logical separation of services/accounts to maintain a secure posture and minimise the risk of published vulnerabilities being exploited

necessary for their role generally referred to as the principle of 'Least Privilege'	
• Suppliers must have suitable and proportional process to identify, assess and mitigate potential Cyber security threats, vulnerabilities in a timely manner	• Policy, process and technology is in place for the management of mobile devices (including any use of mobile storage devices). No portable media (smartphones, tablets and laptops) or storage devices (e.g. USB drive) are to be used for delivery of this contract without authority from HMRC • For particularly sensitive assets you must also have either Cyber Essentials Plus (CE+) or ISO 270001. For ISO 27001 this must be certified by a UKAS accredited company
What, if any, form of assessment in relation to the Cyber Essentials Scheme has been performed, including CE+ and attach the latest certificates that confirm the validity and scope of the certification. If no assessment has been performed, please state when you expect it to be completed.	
REDACTED	
What security accreditation does your organisation currently possess, such as, but not exclusive to ISO27001 and PCI DSS. Please attach the latest current certificate that confirms both the validity and scope of any accreditation.	
REDACTED	

Please provide details of the controls and processes you have in place covering: ● Malware including content inspection on files and messages ● Boundary/network security ● Content checking/blocking (filters) ● Security Incident Management ● Suitable vulnerability management process to manage security patching and vulnerabilities, how regularly the patching is updated. E.g. Patch Tuesday / out of band alerts ● Lockdown (prevention) ● How regularly these are updated
REDACTED
Please provide details of the following access controls: ● Formal registration/deregistration process for users, and ● Users authorisation, authentication process ● Please also include details of the measures in place to manage privilege access (principle of least privilege). e.g. system administrators and remote access usage
REDACTED
Please provide details of: ● Use and control of back-up systems (including cloud solutions) ● Network storage and segregation of HMRC data from other client's data for both paper and electronic data (including 'cloud' solutions) ● Additional security layers for more sensitive information assets ● Location of HMRC data (including offices as well as support / cloud solutions / data centres / backup or disaster recovery options). Please note that if any HMRC data is processed, accessed, stored, backed up or viewed outside the UK you will need to go through HMRC's offshoring approval process.
REDACTED

How will you ensure all software is approved before being installed, and how will ongoing changes to software installation and updates be managed.
REDACTED
Please provide the date when the last penetration test was carried out, and whether this was carried out by a CHECK approved company (NCSC).
REDACTED
Please confirm that you have addressed any risks identified from the penetration test and how this was carried out.
REDACTED
If HMRC has approved the use of portable electronic equipment (e.g. tablets, laptops and mobile phones) or any storage devices (e.g. USBs), please provide details of the controls and processes (including level of encryption and controlled access procedures) you have in place.
REDACTED
How will all equipment (e.g. hardware, laptops, portable media) that holds or has held data be destroyed or decommissioned, and how all data will be rendered unreadable and irretrievable in line with the government's Security Policy Framework. Please also state how you will dispose of any paper assets or electronic data, and how you conform to industry standards for any destruction and disposal processes?
REDACTED

How do you keep up to date with current security threats and risks? Please include product development, knowledge, operational, as well as Cyber.
REDACTED
How is data in transit protected between your end user device(s) and the service - please include the standard of encryption used. Where encryption keys are used please explain who manages these.
REDACTED
How do you protect any data at rest, and include the standard of encryption used
REDACTED

Data Protection Requirements	
High Level Requirements	**Supporting Requirements**
• You must demonstrate GDPR / DPA 2018 compliance (see below) • ICO Contracts Guidance	• Staff training and awareness on data protection / GDPR principles for those staff who have access to HMRC personal data • You must have appropriate data handling arrangements in place e.g. access controls and storage, retention and disposal appropriate to the data sensitivity and format

• CCS PPN 02/18	
• You must have organisational and technical measures to protect against accidental or malicious loss, destruction, damage, alteration or disclosure of HMRC personal data	• Documented and embedded information management policies and processes such as information asset registers, retention and deletion schedules • Agreed Subject Access Request (SAR) / data rights request process
• You must demonstrate how you manage, control and audit access to any HMRC personal data, including protection for special category data	• HMRC data must be stored, accessed, processed, viewed or backed up within the UK, unless prior approval is obtained from HMRC • Clear understanding of the controller and processor roles with regards to HMRC data

Please advise what steps you have taken to ensure compliance since the GDPR / DPA 2018 regulations were introduced. Please explain how you comply with each of the 7 supporting principles, namely: I - Staff training and awareness on data protection II - Data handling arrangements, including access controls and the decommissioning / destruction of personal data and the equipment on which it is held. The HMG Security Policy Framework refers III - Information management policies, processes, documentation including information asset registers, retention and disposal schedules and how these are applied IV - Provide details of the technical and organisational measures you have in place (include areas such as segregation of duties, access/user role management and systems audits/logging) to protect against accidental or malicious damage to HMRC personal data V - Your SARs / Data Rights Request Process VI - Confirmation of where HMRC data for this service is stored, processed, backed up, accessed, viewed from VII - Confirmation of your role as a processor or controller
REDACTED
Please provide a copy of your GDPR privacy notice and advise how regularly you review it
REDACTED

Have the ICO ever issued you with any enforcement notice? Please indicate yes or no. If yes, please provide details and any actions you have taken to address the issues.
REDACTED

Sub-Contractors Requirements	
High Level Requirements	**Supporting Requirements**
• Third party suppliers / sub-contractors must be contractually subject to the same security requirements in all aspects of contract delivery namely security accreditation, physical, personnel, Cyber security, data protection, incident management and business continuity management	• You must have a robust process for ensuring any third party suppliers / sub-contractors used in delivering the HMRC contract meet the minimum standards required • You must have an ongoing assurance process to ensure compliance with standards is maintained

Please confirm your organisation and any third party suppliers / sub-contractors will conform to the requirements set out in the Government Security Policy Framework and any Security requirements recorded in the schedules and/or Order Form?
REDACTED
If you intend to involve third party suppliers / sub-contractors at any stage during the Contract please list them where known, and explain what part of the service they will deliver.
REDACTED
How will you ensure initial compliance and ongoing assurance in your supply chain (where there is a supply chain) with HMRC's security requirements?
REDACTED
How will you ensure the sub-processors meet GDPR / DPA2018 requirements where appropriate, including the controls and documentation used.
REDACTED

Security Incident Management Requirements	
High Level Requirements	**Supporting Requirements**
• Arrangements must be in place for reporting to HMRC any incident which impacts on the	• HMRC must be notified as soon as possible of discovery of an incident, and no later than within two working days. • You must have a process in place for reporting and managing security incidents both within your organisation and to HMRC, including potential ICO notifications

services provided, including cyber security incidents	
HMRC expects to be notified within 24 hours of any security incident that does or could affect our data or the services you provide. What are your processes and timescales for reporting security incidents to HMRC, including the names, role and contact details of the responsible person(s) who will do this?	
REDACTED	

Business Continuity Management Requirements	
High Level Requirements	**Supporting Requirements**
• Third party suppliers must have business continuity and disaster recovery plans in place, aligned with recognised industry standards	• You must have a process in place to assess risks to operations that may impact on delivery of the service to HMRC • You must produce and maintain business continuity and disaster recovery documentation. (business continuity planning is the ability of an organisation to maintain essential functions during, and after a disaster has occurred. Disaster recovery is a set of policies, tools and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a disaster) • A desktop business continuity exercise / test must be run as a minimum once every 12 months. Confirmation to HMRC is required that this activity has been completed, including any observations/mitigation plans that could impact on HMRC assets • Ideally, you will have ISO22301 certification, with an ongoing assurance programme. Please attach if this is the case

Please describe your organisation's business continuity and disaster recovery plans / arrangements in terms of the HMRC data under the contract.
REDACTED
Do you operate any aspects of business continuity or disaster recovery from outside the UK? (If you do you must go through HMRC's offshoring approval process as per the Mandatory Security section).
REDACTED
How frequently are business continuity and disaster recovery plans tested?
REDACTED
When were they last tested, and are the results of testing exercises available for review if requested?
REDACTED
How do you assure continuity of your supply chain?
REDACTED