SCHEDULE 2.4

SECURITY MANAGEMENT

Security Management

1. DEFINITIONS

In this Schedule, the following definitions shall apply:

"Breach of Security"	the occurrence of: (a) any unauthorised access to or use of the Services, the Authority Premises, the Sites, the Supplier System, the Authority 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 each case as may be more particularly set out in the security requirements in Schedule 2.1 (Services Description) and the Baseline Security Requirements;
"CESG"	the UK Government's national technical authority for information assurance;
"CPA"	the CESG Commercial Product Assurance scheme;

"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;

2. SECURITY REQUIREMENTS

2.1 The Supplier shall comply with the Baseline Security Requirements and the Security Management Plan and the Supplier shall ensure that its Security Management Plan fully complies with the Baseline Security Requirements and the Security Policy Framework.

2.2 The Authority shall notify the Supplier of any changes or proposed changes to the Baseline Security Requirements.

2.3 If the Supplier believes that a change or proposed change to the Baseline Security Requirements will have a material and unavoidable cost implication to the Services it may submit a Change Request. In doing so, the Supplier must support its request by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs. Any change to the Charges shall then be agreed in accordance with the Change Control Procedure.

2.4 Until and/or unless a change to the Charges is agreed by the Authority pursuant to the Change Control Procedure the Supplier shall continue to perform the Services in accordance with its existing obligations.

3. PRINCIPLES OF SECURITY

3.1 The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Services, confidentiality, integrity and availability of information and consequently on security.

3.2 The Supplier shall be responsible for the effective performance of its security obligations and shall at all times provide a level of security which:

(a) is in accordance with the Law and this Agreement;

(b) as a minimum demonstrates Good Industry Practice;

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

(d) complies with the Baseline Security Requirements and the Authority's specific security requirements as described in the Services Description as appropriate.

3.3 In the event of any inconsistency in the provisions of the standards, guidance and requirements listed in Paragraph 3.2 above, the Supplier should notify the Authority's Representative of such inconsistency immediately upon becoming aware of the same, and the Authority's Representative shall, as soon as practicable, advise the Supplier which provision the Supplier shall be required to comply with.

4. MALICIOUS SOFTWARE

4.1 The Supplier shall, as an enduring obligation throughout the Term and at no cost to the Authority, use the latest versions of anti-virus definitions and software available from an industry accepted anti-virus software vendor (unless otherwise agreed in writing between the Parties) to check for, contain the spread of, and minimise the impact of Malicious Software in the IT Environment (or as otherwise agreed by the Parties). The Supplier may be required to provide details of the version of anti-virus software being used in certain circumstances, e.g. in response to a specific threat.

4.2 Notwithstanding Paragraph 4.1, if Malicious Software is found, the Parties shall co-operate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Authority Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.

4.3 Any cost arising out of the actions of the Parties taken in compliance with the provisions of Paragraph 4.2 shall be borne by the Parties as follows:

(a) by the Supplier where the Malicious Software originates from the Software (except where the Authority has waived the obligation set out in Paragraph 4.1) or the Authority Data (whilst the Authority Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Authority when provided to the Supplier; and

(b) otherwise by the Authority.

5. SECURITY MANAGEMENT PLAN

5.1 Within twenty (20) Working Days after the Effective Date, the Supplier shall prepare and submit to the Authority for approval in accordance with Paragraph 5.3 a fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of Paragraph 5.2.

5.2 The Security Management Plan shall:

(a) be based on the Supplier's final response to the Authority's Security Questionnaire, a copy of which is set out in Annex 2;

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

(c) 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;

(d) 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;

(e) 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;

(f) set out the plans for transiting all security arrangements and responsibilities for the Supplier to meet the full obligations of the security requirements set out in Schedule 2.1 (*Services Description*) and this Schedule;

(g) 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.

5.3 If the Security Management Plan submitted to the Authority Representative pursuant to Paragraph 5.1 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 5.3 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 5.2 shall be deemed to be reasonable.

5.4 Approval by the Authority of the Security Management Plan pursuant to Paragraph 5.3 or of any change or amendment to the Security Management Plan shall not relieve the Supplier of its obligations under this Schedule.

6. AMENDMENT AND REVISION OF THE SECURITY MANAGEMENT PLAN

6.1 The 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 Services and/or associated processes;

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

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

6.2 The Supplier shall provide the Authority with the results of such reviews as soon as reasonably practicable after their completion and amend the 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 Security Management Plan;

(b) updates to the risk assessments;

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

6.3 Subject to Paragraph 6.4, any change which the Supplier proposes to make to the Security Management Plan (as a result of a review carried out pursuant to Paragraph 6.1, an Authority request, a change to Schedule 2.1 (*Services Description*) or otherwise) shall be subject to the Change Control Procedure.

6.4 The Authority may, where it is reasonable to do so, approve and require changes or amendments to the 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.

7. BREACH OF SECURITY

7.1 Either Party shall notify the other in accordance with the agreed security incident management process (as detailed in the Security Management Plan) upon becoming aware of any Breach of Security 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 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) prevent a further Breach of Security or attempted Breach of Security in the future exploiting the same root cause failure; and

(iv) 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);

(b) as soon as reasonably practicable provide to the Authority full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Authority; and

(c) maintain auditable records of such Breach of Security in accordance with Schedule 8.2 (Reports and Records).

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 Security Management Plan 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 Security Management Plan shall be at no cost to the Authority.

ANNEX 1: BASELINE SECURITY REQUIREMENTS

1 Higher Classifications

1.2 The Supplier shall not handle Authority information 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).

2.3 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 Although the Supplier does not currently meet the government backed Cyber Essentials accreditation criteria in all respects, the Authority is satisfied that their technical controls are aligned closely enough to the requirements as to be acceptable for the provision of the services. The Supplier will alert the Authority immediately should they identify any deterioration or lowering of their technical standards which would result in any further deviation from the recognised Cyber Essentials requirements

3.2 The Supplier and Authority recognise the need for the Authority's information 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 data may be stored, processed and managed from, and what legal and regulatory frameworks Authority information will be subject to at all times.

3.3 The Supplier shall agree any change in location of 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 transfer of Personal Data to a location outside the UK, shall only be given if a Change Request is expressly permitted by Paragraph 1.8 of Schedule 2.8 (*Data Processing and List of Sub-processors*).

3.4 The Supplier shall:

(a) provide the Authority with all Authority Data on written request 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 Information.

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 Authority may request, on a case by case basis, that for certain Supplier personnel roles, additional specific government clearances (such as Security Clearance) are obtained (for example system administrators with privileged access to IT systems which store or process Authority Data). Should staff be identified in roles where the requirement for SC is relevant the Authority may request the additional clearances using the Change Control procedures

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.

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 8.1 for a period of at least six (6) months.

HMRC Standard Goods and Services Model Contract v1.0

ANNEX 2: SECURITY MANAGEMENT PLAN

Background
The Contractor is required to prepare a Security Plan in accordance with the HMRC's Security Policy. The requirements set out in this Security Plan also apply to any sub-contractors engaged by the Contractor to perform any of the services under the Contract. HMRC has developed a standard set of questions and recommendations (see attached Appendices) to ensure consistency across relevant contracts. The Contractor is required to provide answers to the standard set of questions contained within this questionnaire to formulate the initial Security Plan. This Security Questionnaire covers the principles of protective security to be applied in delivering the services in accordance with HMRC's Security Policy and Standards The Contractor's response to this questionnaire, with any subsequent amendments as may be agreed as part of a clarification process, will be included in the signed version of any resulting agreement, as confirmation that the content of the Security Plan has been agreed with HMRC. Bottomline answers in Red for each question.
1 Policy & Standards
1a Please confirm 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
1b Please confirm your organisation and any subcontractors' will conform to the requirements set out in the Government Security Policy Framework (SPF), available from www.gov.uk and any Security Requirements recorded in the schedules and/or Order Form. Redacted
1c If you believe that the Public Sector Network (PSN) Code of Connection, available from www.gov.uk, will apply to your organisation and any sub-contractors, please provide details of how you will conform to this. Redacted
1d Please confirm that your organisation and any sub-contractors will handle HMRC assets in accordance with legislation including the General Data Protection Regulation see GDPR and in accordance with Clause 23 (Protection of Personal Data) of the Contract. Redacted

1e Please also confirm your Data Protection registration number. More information can be found via the following link: Information Commissioners Office see www.ico.org.uk Redacted
1f 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 and describe the process used to achieve the accreditation. Redacted
1g If you intend to involve sub-contractors at any stage during the Contract please list them and explain what part of the service they will deliver. Please also provide details of how you will ensure their compliance with all aspects of this Security Plan. Redacted
1h 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
2 Physical Security (For requirements please see Appendix A – Physical Security)
2a For the locations where HMRC assets are held please provide details of any procedures and security in place designed to control access to the site perimeter. Detail measures such as fencing, CCTV, guarding, and procedures and controls in place to handle staff and visitors requesting access to the site. Please also provide details of the maintenance schedule of your security controls. Redacted
2b Please provide details of the building where the service will operate from and describe the procedures and security in place to control access to premises and any areas within the premises holding HMRC assets. Detail measures such as building construction type, availability of lockable storage, procedures covering end of day/silent hours, key management, visitor controls. Please also include details of any automated access controls, alarms and CCTV coverage. Please also provide details of the maintenance schedule of these security controls. Redacted .

3 IT Security (For requirements please see Appendix B – IT Security)

3a Please state what, if any, form of assessment in relation to the Government backed Cyber Essentials Scheme has been performed or provide details of any cyber essentials accreditation that you are planning in the future.

Redacted

3b 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
- How are external interfaces protected against intrusion?
- How is Malware dealt with?
- Lockdown (prevention)
- How regularly these are updated
- How the service is continually monitored/tested to ensure it remains secure?
- How the service is audited

Redacted

3c Please provide details of the overall security and access control policy of your systems covering physical and electronic assets (including communications connection equipment, e.g. bridge, routers, patch panels). You should record details of the formal registration/deregistration process, how users are Authorised, Authenticated and held Accountable for their actions. Also include details of the measures in place to manage privilege access e.g. System Administrators and remote users and how this is audited and checked.

Redacted

3d Please provide details of how your security and access control policy complies with the Security Policy Framework (including where necessary, use and control of backup systems, network storage and segregation of HMRC data (including 'cloud' solutions), and additional security for more sensitive information assets).

Redacted

3e How is data in transit protected between your end user device(s) and the service. Where encryption keys are used please explain who manages these. Redacted
3f Please describe how you ensure all software and data is approved before being installed, and how your information systems are reviewed for compliance with security implementation standards (e.g. penetration testing - how frequently and are they performed by a CHECK certified professional?). Redacted
3g How do you protect any data at rest? If so how? (Please include details of how internal access is controlled monitored and assured.) Redacted
3h Please provide details of the controls and processes (including level of encryption and controlled access procedures) you have in place for the use of portable media and storage devices exceptionally loaded with HMRC data. Redacted
3i Please provide details of how all equipment (e.g. hardware, portable media) that holds or has held data will be destroyed or decommissioned, and how all data will be rendered unreadable and irretrievable in line with HMG Security Policy Framework requirements for information management. Redacted
3j What Physical protection is in place to stop tampering, theft, or reconfiguration of systems? Redacted
3k How is the service hardened? Redacted
4 Personnel Security (For requirements please see Appendix C – Personnel Security)

4a Have all staff who will have access to, or come in to contact with HMRC data or assets undergone Baseline Personnel Security Standard checks (See www.gov.uk for further information). Redacted
4b Please provide details of how you will 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
4c All contractor's personnel who have access to HMRC data, and/or are directly involved in the service provision must sign a copy of HMRC's Confidentiality Agreement. Please confirm that, in the event that your bid is successful, you will provide signed hard copies of the CA for all personnel involved in this Contract if requested. Redacted
4d Please provide details of the ongoing training you provide to staff in respect of data security, including risk awareness and the identification and reporting of security incidents. Please also provide details of your documented information security procedures and processes that are available to all staff who will have access to, or come into contact with HMRC data. Redacted
4e Please provide details of your procedures for on and off boarding staff Redacted
5 Process Security (For requirements please see Appendix D – Process Security)
5a Please provide details of the format in which HMRC data will be held, how you will ensure segregation of HMRC data, and the locations where this data will be processed. Redacted
5b Please confirm your understanding and agreement that the transfer of any HMRC asset to third parties (any individual or group other than the main Contractor) is prohibited without prior written consent from HMRC. If you anticipate transferring data, especially using portable media during the delivery of this project, please set out your proposed transfer procedures for consideration.

Redacted
5c Please confirm that you understand that HMRC data must not be processed or stored outside the United Kingdom without the express permission of HMRC. If you are considering storing or processing data outside of the UK, please provide details on how and where the data will be stored and also provide details of how you comply with Cabinet Office policy for offshoring see www.gov.uk Redacted
5d In order to protect against loss, destruction, damage, alteration or disclosure of HMRC data, and to ensure it is not stored, copied or generated except as necessary and authorised, please provide details of the technical and organisational measures you have in place (including segregation of duties and areas of responsibility) to protect against accident or malicious intent. Redacted
5e What arrangements are in place for secure disposal of HMRC assets that may be in your possession once no longer required? Redacted
5f How and when will you advise HMRC of security incidents that impact HMRC assets that may be in your possession? Redacted
5g Please describe your disciplinary procedures in the event of a security breach involving HMRC data. Redacted
5h Do you have a List X accreditation? Redacted If 'yes', please answer the following: • What is the name of your Security Controller? • What/Where does the List X accreditation cover? • For what purpose?

- Please provide evidence the Department who sponsored the List X accreditation has agreed to share the environment.

6 Business Continuity

6a Details of the required priority timings/incident types etc. for this service provision have been provided as an attachment to this event entitled 'Business Continuity Grid V0.2 Example' please confirm your understanding and provide an overview of your organisation's Business Continuity and disaster recovery plans in terms of the HMRC data under the Contract. Please specify if you operate business continuity or disaster recovery from offshore.
Also, please provide details on when and how frequently these plans are tested and advise when they were last tested and confirm that results of testing exercises are available for review if requested. Please provide details on how you will meet any recovery times recorded in the Schedules and/or Service Order Form.

Redacted

6b Please confirm that you will comply with all of the specific requirements expressed in Sections 2, 3, 4 and 5 of Schedule 8.6 (Business Continuity and Disaster Capability) relating to the provision of a detailed Business Continuity and Disaster Capability (BCDC) Plan in respect of all the Services that are to be provided under the terms of the Contract.

Redacted

6c In respect of all the Services that are to be provided under the terms of the Contract, please (a) confirm that you will comply with the various requirements specified in Section 6 and Section 7 of Schedule 8.6 (Business Continuity and Disaster Capability) relating to regular review and testing of the Business Continuity and Disaster Capability Plan and (b) provide a description of the proposed frequency, scope and content of the BCDC Plan testing process or programme.

Redacted

6d Please confirm that you will comply with the requirements expressed in Section 8 of Schedule 8.6 (Business Continuity and Disaster Capability) relating to immediate invocation of the BCDC Plan (and prompt notification of HMRC/the Authority) in the event of a complete loss of service or in the event of a Disaster**.**

Redacted

7 Cryptography

7a Please provide details of processes and procedures in place for handling Government cryptographic material. (If this applies)

Redacted

The following appendices provide additional information on the types of security control that <u>may</u> be expected as a minimum for the protection of HMRC information, data and assets.
It is not a legally binding document, nor does it provide a definitive list of baseline security controls. It Should be read in conjunction with HMG and HMRC Security Policy and Standards.

Appendix A – Physical Security

Please consider: the effect of topographic features and landscaping on perimeter security; the possibility of being overlooked; the ease of access and communications; the existence and proximity of public rights of way and neighbouring buildings; the existence of emergency and evacuation routes from adjacent buildings; the implications of shared accommodation; the location of police and emergency services; the build of the structure.

Building Security - There should be as few points of exit and entry as possible but in line with Health & Safety and Fire Regulations. Where exit and entry points exist then physical security controls, such as window bars, grilles shutters Security Doors etc may be installed. The effectiveness of these protection measures may be enhanced by the use of Intruder Detection Systems (IDS), CCTV or Guard Service.

Physical Security	Requirements	Recommended
Secure Rooms	Construction in line with CPNI guidance; locked during 'silent hours' and keys/combinations secured. Sufficient CPNI-Approved lockable storage for material at OFFICIAL or above. Intruder alarm with key holder response.	Intruder alarm with police response. Appropriate automated access control system.
Perimeter Security		CCTV Coverage to identify intruders with adequate lighting for night-time operation. Use of fencing that offers a degree of resistance to climbing and to deter an opportunist e.g. anti-intruder fencing. Manned guarding to be considered.

Physical Security	Requirements	Recommended
Physical Access - secure areas	Visitors limited to those with a business need, issued with identifying badges upon arrival and escorted at all times.	A visitor log maintained and visitors sign in and out.
Building	Constructed of robust building materials typically, brick or lightweight block walls. External doors of solid construction, locked during silent hours and linked to intruder detection system. Access to keys must be checked and any lock combinations changed at regular intervals not exceeding 12 months. A record of key/combination holders must be maintained. The number of keys to a lock must be kept to a minimum. Spare keys must not be held in the same container as 'working keys'. The premises must be locked during 'silent hours' and keys secured. Intruder alarm with key holder response. Windows double glazed or similar unit with locks. Emergency exit doors included on intruder detection system.	Security Keys should not be removed from the premises. Intruder alarm with police response. Power outage alarm with key holder response. Appropriate automated access control system.
Environmental	Fire risk assessment must be carried out. Uninterruptible power supply for security and health & safety equipment.	Smoke detection system e.g. VESDA.
Transport and Storage	Appropriate CPNI-Approved lockable storage for HMRC material. Point to point transfer of all HMRC material using CPNI-Approved locked containers and (where necessary) solid sided vehicles.	HMRC "trusted hand" using named individuals.

Appendix B – IT Security

IT Security	Requirements	Recommended
Cyber Essentials	It is **mandatory** for HMG suppliers to demonstrate that they meet the technical requirements prescribed by Cyber Essentials.	Cyber Essentials Plus with independent assessment and certification.
Authorisation	Users and Administrators must be authorised to use the System/Service. Higher privilege access accounts should be tightly controlled and only assigned to authorised individuals.	
Authentication[1]	Individual passwords must be used to maintain accountability; Robust passwords should be used, that are designed to resist machine based attacks as well as more basic guessing attacks. Passwords must be stored in an encrypted form using a one-way hashing algorithm. Passwords must be able to be changed by the end user, if there is suspicion of compromise. Passwords must be changed at least every 3 months.	Machine-generated passwords. Multi-factor authentication should be considered for exposed environments and remote access. Passwords for privileged accounts/users (Administrators) etc. should be changed more frequently than every 3 months.
Access Control	User access rights to HMRC information assets must be revoked on termination of employment. Audit logs for access management in place showing a minimum of 30 days of activity.	
Malware Protection[2]	Malware protection software should be installed on all computers connected or able to connect to the Internet. It must be regularly updated in line with vendor recommendations or at least daily and should be configured to	Consideration should be given to allowing privilege users (System Administrators) to only use a limited 'non-privilege role' to conduct vulnerable operations such as browsing or importing via removable media.

[1] Authentication is the process by which people "prove" to the system that they are the person they claim to be. There are three possible authentication factors: Passwords (something a person knows), tokens (something a person possesses), and biometrics (something a person inherently is or how they behave).

[2] CESG Good Practice Guide No 7 provides information on the threats and vulnerabilities and risks associated with malicious code and also provides guidance on appropriate risk management measures.

IT Security	Requirements	Recommended
	scan files on access and perform regular scans of all files at server and desktop level (PC/Laptop etc). It should also be configured to identify and block access to known malicious websites. Security Operating Procedures (SyOps) must ensure that malware protection is kept up to date. Anti-Virus Administrators and users should be trained on use of AV software. Users should receive awareness training so that they are aware of risks posed by malicious code from the use of email and attachments, internet and removable media (CD, DVD, USB devices etc). All users, systems and services must be provided on a least privilege basis to reduce the potential for accidental introduction of malicious code. For systems attaching to HMRC network, dual layered malware protection and detection capability.	Dual layered malware protection and detection capability. Malware protection software should be configured to update automatically or update through the use of a centrally managed deployment. Systems and services holding assets with a Government Security Classification of Secret are expected to be air-gapped and will therefore require malware protection to be configured manually.
Network Security	Information, applications and computers within the organisation's internal networks should be protected against unauthorised access and disclosure from the internet, using boundary firewalls, internet gateways or equivalent network devices. Boundary controls should have content checking and a blocking policy in place e.g. firewalls. As a minimum the default administrative password for network devices such as Firewalls should be changed to a strong password comprising of a minimum of 8 characters. All unnecessary services should be disabled/'blocked' by default at the boundary firewall. It is important that Firewall rules that are no longer required are disabled/removed timeously, for example when a service is no longer required.	Dual paired firewalls, different vendors. Anomaly detection capability e.g. Network intruder detection system.

IT Security	Requirements	Recommended
	The administrative interface used to manage boundary firewall configuration routinely must NOT be accessible from the Internet.[3]	
Patch Management	Software should be patched and devices, systems, operating systems and applications should be 'locked down' to remove unnecessary services and functionality. File types should be limited. All Critical security patches should be deployed timeously and in line with vendor recommendations. The deployment of Important i.e. less critical patches should be deployed on the basis of risk.	
System Documentation	System designs/architectural blue prints and network designs should be protected from unauthorised access, loss and destruction.	
Disposal of media	HMRC information assets must be sanitised in line with HMG IA Infosec Standard 5 Secure Sanitisation. Your CESG contact can provide further information.	
Technical Testing	IT health check aka penetration testing for front facing internet services delivered to HMRC.	Consideration for regular IT health check of application and infrastructure services delivered to HMRC.
Use of Laptops and removable recordable media.	Laptops holding any information supplied or generated as a consequence of a Contract with HMRC must have, as a minimum, a FIPS 140-2 approved full disk encryption solution installed. Approval from HMRC must be obtained before information assets are placed on removable media[4]. This approval must be documented sufficiently to establish an audit trail of responsibility. All removable media containing information assets must be encrypted. The level of encryption to be applied is determined by the highest HM Government Security	

[3] It is envisaged that systems holding Secret assets will not be supported by a remote administrative and will not be Internet facing.

[4] The term drives includes all removable, recordable media e.g. memory sticks, compact flash, recordable optical media and external hard drives.

IT Security	Requirements	Recommended
	Classification of an individual record on the removable media. Unencrypted media containing HMRC information assets must not be taken outside secure locations; the use of unencrypted media to store HMRC information assets must be approved by HMRC.	

Appendix C – Personnel Security

Personnel Security	Requirements	Recommended
Security Clearance	Pre-employment checks should meet the Baseline Personnel Security Standard (BPSS) and must be completed for all staff with potential or actual access to HMRC assets. Security Clearance for all staff with access or potential access to material with a Government Security Classification of SECRET.	See www.gov.uk specifically the link to the Disclosure & Barring Service for more information. Staff with privileged system access (system administrators) to have Developed Vetting Clearance.
Confidentiality Agreements	Confidentiality Agreements (CA) must be completed by all staff with potential or actual access to HMRC information assets as requested.	
Security Awareness Training	All staff must undergo security awareness training and be familiar with HMRC security policy, standards and guidance. There must be a plan in place, endorsed and owned by a named individual at Board Level, to ensure refresher training takes place at least annually.	Board members and senior management should be able to demonstrate their commitment to security through a variety of mechanisms.
Joiners and leavers	Process to ensure individuals are appointed to clearly defined roles with appropriate access rights only. Leavers' access rights to systems and premises are removed on termination of employment.	

Appendix D – Process Security

Process Security	Requirements	Recommended
Disciplinary Process	There must be an organisational disciplinary process. Staff must be briefed on this and the penalties that may result from failure to comply with documented security policies	
Security Policies, Processes and Procedures	Where the contract requires you to hold HMRC assets at Secret or above you MUST ensure there is a relationship at senior management level between your organisation and CESG. Procedures in place to determine whether any compromise of HMRC assets e.g. loss or modification of information, software and hardware has occurred. Procedures for the handling and storage of HMRC information assets must be established to protect from unauthorised disclosure and/or misuse. End of day procedures must ensure that HMRC assets are adequately protected from unauthorised access. A clear desk policy must be enforced. Procedures must be in place to ensure HMRC's assets are segregated from any other Client's assets held by the contractor. Procedures for the secure disposal of the HMRC's assets must be in place. Where HMRC assets are held at SECRET all staff and visitors must visibly wear an identifying pass while on site. Where HMRC assets are held at SECRET portable media devices must be excluded from the secure area. A challenge culture must be fostered, so that staff or visitors not wearing a pass are challenged. Where an access control system is in operation tailgating must be discouraged.	Obtain the services of a CLAS consultant to help you through the bidding process and, if successful, the early stages of contract award.

Process Security	Requirements	Recommended
	Where required HMRC assets must be destroyed in line with the Security Policy Framework. Further guidance on storage and destruction of media is available from CESG.	
Transfer of HMRC Data	Any proposed transfer of HMRC data must be approved by HMRC in writing. If the Contractor is unsure whether approval has been given, the data transfer must not proceed. Where data transfers are necessary in the performance of the Contract, they should be made by automated electronic secure transmission via the Government Secure Internet (GSI) with the appropriate level of security control. Individual data records (unless as part of a bulk transfer of an anonymised respondent survey data) will require specific transfer arrangements. Transfer of aggregated data such as results, presentations, draft and final reports may also need discussion and agreement, again in advance of any such transfer.	**Whenever possible, putting data on to removable media should be avoided.** Where this is unavoidable, hard drives and personal digital assistants, CD-ROM/DVD/floppy/USB sticks are only to be used after discussion and agreement with HMRC in advance of any such transfer. If the use of removable media is approved, data must be written to them in a secure, centralised environment and be encrypted to HMRC's standards. If you anticipate transferring data on removable media during the delivery of this project please set out your proposed transfer procedures.
Incident Management	Arrangements must be in place for reporting security breaches to the asset owner.	
List X	Further information on List X is available at www.gov.uk. A List X accreditation may just cover a floor, a room or even a particular piece of secure furniture and may be for a specific purpose. Note: If you do have a List X accreditation, please keep responses generalised for the purposes of completion of this question.	

Appendix E – Business Continuity

Business Continuity Requirements	Requirements	Recommended
Business Continuity Management	3rd party suppliers should provide HMRC with clear evidence of the effectiveness of its Business Continuity management arrangements and alignment with recognised industry standards, by assessing risks to their operations and producing and maintaining business continuity documentation.	

Appendix F – Cryptography

Government Cryptography	Requirements	Recommended
Cryptographic Material	Information on this subject will be available from your contact in CESG.	

Annex 3 - Bottomline Security Policies

Standard/Policy	Filename	Version No.	Date	Notes
Cyberfort (Bunker) Factsheet	Secure Location.pdf	-	Jul-21	Marketing Brochure - no version control
Physical Security Standard	Physical Security Standard	2.3	Dec-20	

FML Business Continuity Plan	FML Busines Continuity Plan 4.6_redacted.pdf	4.6	Dec-20	
Bottomline Information Security Policies	Bottomline Information Security Policies		Dec-20	Reviewed, approved and signed by CISO on annual basis
Application Security Testing Standard	Application Security Testing Standard	9.2	Jan-21	
Continuity of Operations Standard	Continuity of Operations Standard	2.3	Dec-20	