

**Security Plan Questionnaire - Low**

|  |  |
| --- | --- |
| **To:** |  |
| **From:** |  |
| **Date:** |  |
| **Tender reference:** |  |
| **Tender title:** |  |
|  | |

**Schedule 2.4 Security 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. |
| **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. |
| **1b** Please confirm your organisation and any subcontractors' will conform to the requirements set out in the Government Security Policy Framework (SPF), available from [Security Policy Framework](https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework) and any Security Requirements recorded in the schedules and/or Order Form. |
| **1c** If you believe that the [Public Sector Network (PSN)](https://www.gov.uk/government/groups/public-services-network) 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. |
| **1d** Please confirm that your organisation and any sub-contractors will handle HMRC assets in accordance with legislation including the UK General Data Protection Regulation see UK [GDPR](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/) and in accordance with Clause 23 (*Protection of Personal Data*) of the Contract.. |
| **1e** Please confirm that you have paid the Data Protection Fee to the ICO or that you fall into one of the exempt categories. More information can be found [here](https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/02/new-model-announced-for-funding-the-data-protection-work-of-the-information-commissioner-s-office/) |
| **1f** Please provide details of any security accreditation that your organisation currently possesses, such as but not exclusive to, ISO27001 and PCI DSS and describe the process used for achieving the accreditation. |
| **1g** If you intend to involve sub-contractors at any stage during the Contract please list them and provide details of how you will ensure their compliance with all aspects of this Security Plan. |
| **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. |
| **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 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. |
| **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. If no assessment has been performed please state when you expect it to be completed. |
| **3b** Please provide details of the controls and processes you have in place covering patching, malware (anti-virus), boundary/network security (intruder detection), content checking/blocking (filters), lockdown (prevention), and how regularly you update them. |
| **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. |
| **3d** Please provide details of how your security and access control policy complies with Security Policy Framework requirements including where necessary, use and control of back up systems, network storage and segregation of HMRC data (including 'cloud' solutions), and additional security for more sensitive information assets. |
| **3e** 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). |
| **3f** 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. |
| **3g** 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 the Security Policy Framework. |
| **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](http://www.gov.uk)). |
| **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? |
| **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 (CA). Please confirm that, in the event that your bid is successful, you will provide signed hard copies of the NDA for all personnel involved in this Contract if requested. |
| **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. |
| **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 including any associates/sub-contractors) is prohibited without prior written consent from the 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. |
| **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 transferring data outside of the UK, please provide details on how and where the data will be processed or stored.    To the extent that any data offshoring would include the transfer of Personal Data (as defined in the United Kingdom General Data Protection Regulation (UK GDPR)) outside of the UK, please provide details of the protections and safeguards which would be applied to ensure that such data is afforded a level of protection that is essentially equivalent to that guaranteed in the UK by UK GDPR, including in relation to access to the data by the country’s public authorities.    Please note: In line with HMRC’s current policies, the successful supplier(s) will not be permitted to transfer any Personal Data provided by HMRC in connection with any contract resulting from this procurement exercise to any country outside of the UK where such transferred data will not be afforded a level of protection essentially equivalent to that guaranteed in the UK by UK GDPR.    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 outside of the UK without ensuring the transferred data is afforded a level of protection essentially equivalent to that guaranteed in the UK by UK GDPR. |
| **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. |
| **5e** What arrangements are in place for secure disposal of HMRC assets once no longer required? |
| **5f** How and when will you advise HMRC of security incidents that impact HMRC assets. |
| **6 Business Continuity** (For requirements please see Appendix E – Business Continuity) |
| **6a** Please provide an overview of your organisation’s business continuity and disaster recovery plans in terms of HMRC data under the Contract, or attach a copy of your Business Continuity Plan. |

**The following appendices provide additional information on the types of security control that may 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, and must 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 - Preferably 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** |
| --- | --- | --- |
| Physical Access - secure areas | Visitors should be identifiable and escorted at all times | Visitor to be issued with identifying badges upon arrival.  A visitor log maintained and visitors sign-in and out. |
| Building | Should be constructed of robust building materials typically, brick or lightweight block walls.  External doors should be of solid construction and locked during silent hours.  Access to keys should be checked and any lock combinations changed at regular intervals not exceeding 12 months. A record of key/combination holders should be maintained.  The number of keys to a lock should be kept to a minimum. Spare keys should not be held in the same container as ‘working keys’.  The premises must be locked during ‘silent hours’ and keys secured. | Lockable double glazed or similar unit. Emergency exit doors included on intruder detection system.  Security Keys should not be removed from the premises.  Intruder alarm with keyholder response. |
| Environmental | Fire risk assessment should be carried out.  Uninterruptible power supply for security and health & safety equipment. | Smoke detection system e.g. VESDA. |
| Transport and Storage | Adequate lockable storage for HMRC material.  Material transported using previously agreed processes with HMRC. | Point to point transfer of material in locked containers. |

**Appendix B – IT Security**

| **IT Security** | **Requirements** | **Recommended** |
| --- | --- | --- |
| Cyber Essentials | It is a requirement for HMG suppliers to have undertaken self-assessment and achieved the Government backed Cyber Essentials scheme. | Cyber Essentials Plus with independent assessment and certification. |
| Authorisation | Users and Administrators must be authorised to use the System/Service. |  |
| Authentication[[1]](#footnote-2) | 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. Password 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 | 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]](#footnote-3) | Controls such as anti-virus software must detect and prevent infection by known malicious code.[[3]](#footnote-4)  AV 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).  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.  System designs/architectural blue prints and network designs should be protected from unauthorised access, loss and destruction.  All users, systems and services must be provided on a least privilege basis to reduce the potential for accidental introduction of malicious code.  Application code development should be tightly controlled and subject to strict quality control to reduce the potential for insertion of backdoors that could be exploited by an attacker.  For systems attaching to HMRC network, dual layered malware protection and detection capability. | 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.  Dual layered malware protection and detection capability. |
| Network Security | Boundary controls that have a content checking and blocking policy in place e.g. firewalls. | Dual paired firewalls, different vendors.  Anomaly detection capability e.g. Network intruder detection system. |
| Disposal of media | HMRC information assets must be sanitised in line with the Security Policy Framework. |  |
| 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]](#footnote-5). 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 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** |
| --- | --- | --- |
| Pre-employment checks | 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. | See BPSS, available from ww.gov.uk, specifically the information relating to the Disclosure & Barring Service for more information. |
| Confidentiality Agreements | Confidentiality Agreements (CA) must be completed by all staff with potential or actual access to HMRC information assets as requested. | HMRC’s Commercial Directorate can supply the template form. |

**Appendix D – Process Security**

| **Process Security** | **Requirements** | **Recommended** |
| --- | --- | --- |
| Security Policies, Processes and Procedures | Procedures should be 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 should be established to protect from unauthorised disclosure and/or misuse.  End of day procedures should ensure that HMRC assets are adequately protected from unauthorised access.  A clear desk policy should 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 HMRC’s assets must be in place.  A challenge culture should be fostered, so that unknown staff or visitors are challenged. Where an access control system is used tailgating should be discouraged. | Assets, especially information assets must be destroyed when no longer required so that they cannot be reconstituted or reused by an unauthorised third party. Shedding is recommended. Electronic files should be weeded and deleted when no longer required. |
| 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 the 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 the 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 should be in place for reporting security breaches to the asset owner. |  |

**Appendix E – Business Continuity**

| **Business Continuity Requirements** | **Requirements** | **Recommended** |
| --- | --- | --- |
| Business Continuity Management | 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 |  |

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). [↑](#footnote-ref-2)
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. [↑](#footnote-ref-3)
3. Heuristic scanning capabilities can help detect against previously undocumented attacks but AV products are generally ineffective against day zero attacks and are therefore only effective against known malicious code attacks. It is important therefore that systems and applications are locked down, patched against known vulnerabilities that could allow execution of malicious code e.g. in browsers and email clients. [↑](#footnote-ref-4)
4. The term drives includes all removable, recordable media e.g. memory sticks, compact flash, recordable optical media and external hard drives. [↑](#footnote-ref-5)