## SCHEDULE U: INFORMATION SECURITY

### General

A. In addition to the provisions set out in this Schedule, the Provider shall comply with the provisions relating to Information Security contained in Schedule X (Information Assurance) of this Contract.

### Section I: Security classification and process measures to manage information risk

1.1 The information processed and stored in delivering the Services to the Authority is classified under the Government Security Classifications scheme as OFFICIAL. Some of it may be OFFICIAL- Sensitive. The Provider shall ensure that it and its Sub-contractors apply at least the minimum security controls required for OFFICIAL information as described in Cabinet Office guidance, currently:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf

1.2 In considering the security controls required for the Provider's Systems, the Provider shall demonstrate to the Authority that they have taken into account the "Technical Controls Summary for OFFICIAL" at part 3 paragraph 41 of the above link.

1.3 The Provider and its Sub-contractors shall comply with the HMG Security Policy Framework (SPF) and principles, obligations and policy priorities stated therein. A copy of the SPF can be found on the Cabinet Office website https://www.gov.uk/government/collections/government-security.

1.4 The Provider shall at all times ensure that the level of cyber security and information assurance is maintained to protect the confidentiality, integrity, and availability of information, data and materials used in the provision of the Services and provide acceptable levels of risk management and /or risk acceptance so that the Authority can maintain assurance and accreditation as required by HMG guidance.

1.5 The Cyber Essentials Scheme and the security controls required for OFFICIAL information all complement each other with the aim of achieving sound commercial standards of security in relation to Information and Communications Technology (ICT) and information handling.

1.6 The Provider shall:

1.6.1 identify, keep and disclose to the Authority upon request a record of Users; and

1.6.2 provide to the Authority details of its policy for reporting, managing and recovering from information risk incidents, including losses of protected Personal Data and ICT security incidents and its procedures for reducing risk and raising awareness; and

1.6.3 immediately report information security incidents to the Authority. Significant actual or potential losses of Personal Data may be shared with the Information Commissioner and the Cabinet Office by the Authority.

**Section II: Accreditation and assurance requirements**

2.1 Specific requirements of the assurance and accreditation of IT systems which support the Services are set out below.

Security and IA – Procedural and Policy controls

2.2 The Provider shall develop, implement, operate, maintain and continuously improve an Information Security Management System (ISMS). The ISMS must be aligned to ISO 27001 and/or be certified to ISO 27001.2005 or 27001:2013, and (unless otherwise agreed in writing with the Authority) should be reviewed and tested annually from the Service Commencement Date, or earlier when there is a significant change to the Provider's System. (Note: The Provider may refer to other indicators of good practice such as HMG's 10 Steps to Cyber Security.)

2.3 The Provider's System must comply with applicable Law and relevant HMG security standards.

2.4 The Provider's System must demonstrate procedures for reporting and responding to incidents and for the secure destruction (at the Authority's request) of Authority Data, Information Assets, any other data or information relevant to the provision of the Services and any Hardware or devices on which such data or information is stored.

2.4 Upon request from the Authority and/or any accreditor appointed by the Authority, the Provider shall provide sufficient design documentation detailing the security architecture of its information system and data transfer mechanism to support the accreditor's assurance that it is appropriate, secure and complies with the Authority's requirements.

2.5 The Provider's System shall be assured for handling information classified as OFFICIAL (including OFFICIAL-Sensitive) and be subject to accreditation to HMG standards and meet the standards required for security controls for OFFICIAL information in accordance with the HMG (Cabinet Office and CESG) guidance on Security Technology at OFFICIAL which links to other guidance and references the HMG Security Policy Framework as set out at: https://www.gov.uk/government/collections/securing-technology-at-official.

2.6 The Provider's System shall securely store and process all Authority Data, Information Assets and any other data or information relevant to the provision of the Services recorded on them to comply with HMG Security Policy, Standards and Guidance.

2.7 Where there are aspects of data aggregation, the Authority may require additional security controls above the level of the HMG Baseline in accordance with HMG Security Policy, Standards and Guidance.

Security and IA – Physical and Environmental Controls

2.8 The Provider's systems shall securely store and process all Authority Data, Information Assets and any other data or information relevant to the provision of the Services at least to a standard required at the Government Security Classification OFFICIAL.

2.9 The Provider's System shall be protected by appropriate people, process, technology and physical security controls as part of a 'defence-in-depth' approach.

2.10 The Provider's System should securely identify and authenticate Users before allowing them to access it.

2.11 Where there are aspects of data aggregation, additional controls may be required above the level of the HMG Baseline Controls in accordance with HMG (Security Policy Framework) and Communications-Electronics Security Group (CESG) standards and guidance as set out in paragraph 2.5 of this Schedule U subject to agreement with the accreditor.

2.12 The Provider shall ensure that any electronic transfer of Authority Data, Information Assets or any other data or information relevant to the provision of the Services:

2.12.1 protects the confidentiality of the Authority during transfer through encryption suitable for the impact level of the data or information;

2.12.2 maintains the integrity of the Authority Data, Information Assets and any other data or information relevant to the provision of the Services during both transfer and loading into the receiving system through suitable technical controls for the impact level of the data or information; and

2.12.3 prevents repudiation of receipt through accounting and auditing.

2.13 The Provider shall ensure that all OFFICIAL information is afforded physical protection from internal, external and environment threats commensurate with the Authority's business value of the OFFICAL information.

2.14 All physical components of the Provider's System should be kept in secure accommodation which conforms to HMG (Security Policy Framework) and Communications-Electronics Security Group (CESG) standards and guidance as set out in paragraph 2.5 of this Schedule U and which can be independently audited and approved by the Authority or an Authority Related Party.

2.15 All handling of physical media holding Security Classified (OFFICIAL) Data shall be done in accordance with HMG (Security Policy Framework) and Communications-Electronics Security Group (CESG) standards and guidance as set out in paragraph 2.5 of this Schedule U or equivalent good industry practice.

Security and IA – Technical Controls

2.16 The Provider's System must provide network controls to authenticate internal and external users prior to communicating to prevent unauthorised users gaining access to the Provider's System.

2.17 The import and export of Authority Data, Information Assets and any other data or information relevant to the provision of the Services from the Provider's System must be strictly controlled and recorded / audited.

2.18 The Provider's System must enforce the principle of 'least privilege' and only grant Users the minimum necessary permission to access information / access the service.

2.19 The Provider's System must enforce robust role-based access control mechanisms to prevent unauthorised access to Authority Data, Information Assets or any other data or information relevant to the provision of the Services.

2.20 The Provider's System must implement effective and legitimate monitoring of the Services in accordance with HMG standards, where appropriate, in accordance with CESG Good Practice Guide (GPG) 13 – Protective Monitoring (GPG 13 can be obtained from CESG through a CLAS consultant (https://www.cesg.gov.uk/servicecatalogue/CLAS/Pages/WhatisCLAS.aspx)) or may be provided or summarised by the Authority.

2.21 The Provider shall, where appropriate, ensure that the Provider's System functions in accordance with good industry practice for protecting external connections to the internet.

2.22 The Provider shall ensure that the Provider's System functions in accordance with good industry practice for protection from malicious code.

2.23 The Provider shall ensure that all components of the Provider's System are patched in line with good industry practice and the Provider's patch policy (such patch policy to be agreed with the Authority).

2.24 An ICT health check must be conducted on the Provider's System on an annual basis from the Service Commencement Date by an independent CHECK qualified company if and as required by the accreditor and subject to agreement on its scope between the accreditor and the Provider.

2.25 Technical vulnerabilities of the Provider's System which are identified during the assurance process must be resolved effectively and must be recorded on the system risk register and tracked through the accreditation process where applicable.

2.26 Users must be automatically logged out of the Provider's System if an account / session is inactive for more than 15 minutes. The Provider shall provide to the Authority sufficient design documentation detailing the security architecture of their information system and data transfer mechanism to support the Authority's assurance that the Provider's System is appropriate and secure, and complies with the Authority's requirements.

2.27 The Provider's System must provide network controls to authenticate Users prior to communicating to prevent unauthorised users gaining access to services and information.

2.28 The Provider's System must provide internal processing controls between security domains to prevent the unauthorised high domain exporting of Authority Data, Information Assets or any other data or information relevant to the provision of the Services to the low domain if the solution requires passing data between different security domains.

2.29 Any OFFICIAL-Sensitive data including sensitive Personal Data must be encrypted in transit and when at rest when stored away from the Provider's controlled environment.

2.30 The Provider shall ensure that the Provider's System provides controls to securely manage (store and propagate) all cryptographic keys to prevent malicious entities and services gaining access to them, in line with the Authority's Cryptographic Policy, as made available to the Provider from time to time.

Security and IA – Personnel Controls

2.31 The Provider shall ensure that all its Personnel that have logical or physical access to the Provider's System or Authority Data, Information Assets or any other data or information relevant to the provision of the Services are security cleared to a minimum of "Security Check National Security Vetting".

2.32 The Provider's Personnel that do not have access to the Authority Data, Information Assets or any other data or information relevant to the provision of the Services shall in any event be cleared to the baseline physical security standard or the Provider must

provide evidence that they have controls to prevent these members of the Provider's Personnel from gaining access to the Authority Data, Information Assets or any other data or information relevant to the provision of the Services.

2.33 The Provider must ensure that any of its Sub-contractors are subject to the same security arrangements and meet the same personnel controls and security requirements that are expected of the Provider.

2.34 Procedures should be in place to ensure the Provider's Personnel who have access to Authority Data, Information Assets or any other data or information relevant to the provision of the Services are aware of their responsibilities when handling such data or information and the Provider's System used to process it.

2.35 The Provider's System will support the requirement of the Authority to comply with HMG policy and guidance on Offshoring (https://ogsirooffshoring.zendesk.com/hc/en-us/articles/203107991-HMG-s-Offshoring-Policy) () by assessing, as required, any additional security risks associated with the storage, processing or transmission of data or information offshore, typically by an offshore provider or Sub-contractor (which may include the use of 'landed resources'), taking account of EU requirements to confirm the 'adequacy' of legislated protection of Personal Data in the country(ies) where storage / processing occurs. No element of the Provider's System may be 'off-shored' without the prior Approval of the Authority.

2.36 The Provider shall ensure that its Sub-contractors comply with the provisions of this Schedule U during the provision of the Services, and as may be stated in any data sharing agreement and in the security aspects letter where one is issued by the Authority.

2.37 The Provider shall ensure that effective training and awareness is in place to ensure that all members of the Provider's Personnel are conscious of all information security requirements.

Security and IA – Procedural and Policy Controls

2.38 The Provider shall develop, implement, operate, maintain and continuously improve the ISMS.

2.39 The ISMS must be tested and periodically updated, with a full test, review and update performed at least annually from the Service Commencement Date or when there is a change to the Provider's System, its services and/or associated processes. Where ISO 27001 certification is provided, the ISMS shall be independently audited in accordance with ISO/IEC 27001; and be subject to Approval by the Authority. The certification body must be UKAS accredited.

2.40 The Provider shall have a certified information security policy that reflects the relevant control objectives, including those specified within the ISO27002 control set, for the Provider's System and the services provided.

2.41 The Provider must appoint an ICT system manager or security manager, who is responsible for the provision of technical, personnel, process and physical security aspects for the Provider's System and such individual shall be a member of Key Personnel.

2.42 The Provider's System must comply with applicable Law, relevant HMG security standards and the Authority's security policies.

2.43 The Provider's System must demonstrate procedures for reporting and responding to security incidents comply with arrangements for reporting security incidents to the Authority.

2.44 The Provider's System must demonstrate procedures for the secure destruction (at the Authority's request) as set out at paragraph 3.10 of this Schedule.

2.45 Subject to paragraph 2.1 of Schedule W (Information and Communications Technology) of this Contract, any changes to the Provider's System must be made in accordance with the Change Mechanism set out in Schedule I of the Contract.

**Section III: Specific minimum measures to protect personal information**

3.1 The Provider must be particularly careful to protect Authority Data whose release or loss could cause harm or distress to individuals. The Provider must handle all such Authority Data as if it were confidential while it is processed or stored by the Provider or its Sub-contractors, applying the measures in this Schedule.

3.2 When Authority Data is held on paper it must be kept secure at all times, locked away when not in use on the premises on which it is held and secured. If Authority Data held on paper is transferred it must be by an approved secure form of transfer with confirmation of receipt. When Authority Data is held and accessed on the Authority's System or the Provider's System or any other ICT systems on secure premises, the Provider must apply the minimum protections for information set out in this Schedule the Service Specification (Schedule B), or equivalent measures, as well as any additional protections as needed as a result of the Authority's risk assessment. Where in exceptional circumstances equivalent measures are adopted the Provider must obtain the Authority's prior Approval in writing.

3.3 Wherever possible, Authority Data should be held and accessed on paper, on the Authority's System, on the Provider's System or on other ICT systems on secure premises protected as above. This means the Provider should avoid the use of removable media (including laptops, removable discs, CD-ROMs, USB memory

sticks, PDAs and media card formats) for storage or access to such data where possible. Where the Authority agrees that the best option at paragraph 3.4 below is not possible, the Provider shall consider the Second best option at paragraph 3.5 below and Third best option at paragraph 3.6 below, recording the reasons why a particular approach should be adopted in a particular case or a particular business area and provide this to the Governor seeking the Governor's prior Approval before implementing that approach.

3.4 Best option: hold and access data on the Authority's System, on the Provider's System or on other ICT systems on secure premises.

3.5 Second best option: secure remote access, so that data can be viewed or amended without being permanently stored on the remote computer. This is possible for Authority Data over the internet using products meeting the FIPS 140-2 standard or equivalent, unless otherwise agreed with the Authority,

3.6 Third best option: secure transfer of Authority Data to a remote computer on a secure site on which it will be permanently stored. Both the Authority Data and the link should be protected at least to the FIPS 140-2 standard or equivalent. Protectively marked Authority Data must not be stored on privately owned computers unless they are protected in this way.

3.7 In all cases the remote computer should be password protected, configured so that its functionality is minimised to its intended business use only, and have up to date software patches and anti-virus software.

3.8 Where the Authority agrees that it is not possible to avoid the use of removable media and Approval from the Governor has been obtained as set out at paragraph 3.3 above, the Provider shall ensure compliance with the following conditions:

3.8.1 the Authority Data transferred to the removable media should be the minimum necessary to achieve the business purpose, both in terms of the numbers of people covered by the Authority Data and the scope of Authority Data held. Where possible only anonymised Authority Data should be held;

3.8.2 the removable media should be encrypted to a standard of at least FIPS 140-2 or equivalent in addition to being protected by an authentication mechanism, such as a password;

3.8.3 User rights to transfer Authority Data to removable media should be carefully considered and strictly limited to ensure that this is only provided where absolutely necessary for business purposes and subject to monitoring by the Provider and the Authority; and

3.8.4 the individual responsible for the removable media should handle it – themselves or if they entrust it to others – as if it were the equivalent or a large amount of their own cash.

3.9 Where the Authority agrees that the second condition of encryption in paragraph 3.8.2 cannot be applied due to business continuity and disaster recovery considerations, such unprotected Authority Data should only be recorded, moved, stored and monitored with strong controls.

3.10 All material that has been used for storage of the Authority's Confidential Information should be subject to controlled disposal. The Provider must:

3.10.1 destroy paper records containing protected Personal Data by incineration, pulping or shredding so that reconstruction is unlikely; and

3.10.2 dispose of electronic media that has been used for the processing or storage of protected Personal Data through secure destruction, overwriting, erasure or degaussing for re-use.

3.11 The Provider must have appropriate mechanisms in place in order to comply with the Authority's requirements as set out in this Schedule, including adequate training for the Provider's Personnel in handling Confidential Information.

3.12 The Provider must:

3.12.1 put in place arrangements to log activity of data Users in respect of electronically held protected Personal Information, and for managers to check it is being properly conducted, with a particular focus on those working remotely and those with higher levels of functionality. Summary records of managers' activity must be shared with the Authority and be available for inspection by the Information Commissioner's Office on request; and

3.12.2 minimise the number of Users with access to Authority Data.

## ANNEX A

### Minimum scope of Authority Data which is protected Personal Data

In the absence of specific instructions from the Authority, all the data identified in the table below is data whose release or loss in the Authority's view could cause harm or distress to individuals. The Provider and its Sub-contractors must treat the information identified below as protected Personal Data.

| **1. one or more of the pieces of information which can be used along with public domain information to identify an individual** | **combined with** | **2. information about that individual whose release is likely to cause harm or distress** |
|---|---|---|
| Name/addresses (home or business or both)/post code/e-mail/telephone numbers/ driving licence number/date of birth<br><br>[Note that driving licence number is included in this list because it directly yields date of birth and first part of surname] | | Sensitive personal data as defined by s.2 of the Data Protection Act, including records relating to the criminal justice system, and group membership<br><br>DNA or fingerprints/bank, financial or credit card details/mother's maiden name/National Insurance number/Tax, benefit or pension records/health records/employment record/school attendance or records/material relating to social services including child protection and housing |