Schedule 5

Security Management

Schedule 5: Security Management

Enhanced Security Requirements

GENERAL

The Supplier shall and shall procure that any Sub-contractor (as applicable) shall, comply with the Authority's security requirements as set out in the Contract which include the requirements set out in this Schedule 5 to the Contract. The Authority's security requirements include, but are not limited to, requirements regarding the confidentiality, integrity and availability of Authority Assets, the Authority System and the Supplier System.

Terms used in this Schedule 5 which are not defined below shall have the meanings given to them in Schedule 1 *(Definitions)* of the Contract.

1. DEFINITIONS

1.1 In this Schedule 5, the following definitions shall apply:

"**Authority Personnel**"	shall mean all persons employed by the Authority including directors, officers, employees together with the Authority's servants, agents, consultants, contractors and suppliers but excluding the Supplier and any Sub-contractor (as applicable);
"**Availability Test**"	shall mean the activities performed by the Supplier to confirm the availability of any or all components of any relevant ICT system as specified by the Authority;
"**Breach of Security**"	shall mean an event that results, or could result, in: (a) any unauthorised access to or use of the Authority Data, the Services and/or the Information Management System; 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 Contract;
"Certification Requirements"	shall mean the certification requirements set out in Paragraphs 3.1 and 4.1;
"**CHECK**"	shall mean the scheme for authorised penetration tests which scheme is managed by the NCSC;
"**Cloud**"	shall mean an off-premise network of remote ICT servers on the Internet to store, process, manage and transmit data;
"**Cyber Essentials Plus**"	shall mean the Government-backed, industry-supported scheme managed by the NCSC with higher level of security requirements to help organisations to protect themselves against online threats or the relevant successor or replacement scheme which is published and/or formally recommended by the NCSC;
"**Cyber Security Information Sharing Partnership**" or "**CiSP**"	shall mean the cyber security information sharing partnership established by the NCSC or the relevant successor or replacement scheme which is published and/or formally recommended by the NCSC;
"**Good Security Practice**"	shall mean: (a) the technical and organisational measures and practices that are required by, or recommended in, nationally or internationally accepted management standards and codes of practice relating to Information Security (such as published by the International Organization for Standardization or

the National Institute of Standards and Technology);

(b) security standards and guidelines relating to Information Security (including generally accepted principles regarding the segregation of the duties of governance, implementation and control) provided to the general public or Information Security practitioners and stakeholders by generally recognised authorities and organisations;

(c) the Government's security policies, frameworks, standards, and guidelines relating to Information Security; and

(d) the Authority's security policies, frameworks, standards, and guidelines relating to Information Security; and

(e) compliance with the NCSC 14 Cloud Security Principles;

"**Information Management System**"	shall mean:

(a) those parts of the Supplier System, and those of the Sites, that the Supplier or its Sub-contractors will use to provide the parts of the Services that require Processing Authority Data; and

(b) the associated information assets and systems (including organisational structure, controls, policies, practices, procedures, processes and resources);

"**Information Security**"	shall mean:

(a) the protection and preservation of:

(i) the confidentiality, integrity and availability of any Authority Assets, the Authority System (or any

part thereof) and the Supplier System (or any part thereof);

(ii) related properties of information including, but not limited to, authenticity, accountability, and non-repudiation; and

(iii) compliance with all Law applicable to the processing, transmission, storage and disposal of Authority Assets;

"**Information Security Manager**"	shall mean the person appointed by the Supplier with the appropriate experience, authority and expertise to ensure that the Supplier complies with the Authority's Security Requirements;
"**Information Security Management System" or "ISMS"**	shall mean the set of policies, processes and systems designed, implemented and maintained by the Supplier to manage Information Security Risk as certified by ISO/IEC 27001;
"**Information Security Questionnaire**"	shall mean the Authority's set of questions used to audit and on an ongoing basis assure the Supplier's compliance with the Authority's Security Requirements;
"**Information Security Risk**"	shall mean any risk that might adversely affect Information Security including, but not limited to, a Breach of Security;

"**ISO/IEC 27001, ISO/IEC 27002 and ISO 22301**	shall mean: (a) ISO/IEC 27001; (b) ISO/IEC 27002/IEC; and (c) ISO 22301, in each case as most recently published by the International Organization for Standardization or its successor entity (the "**ISO**") or the relevant successor or replacement information security standard which is formally recommended by the ISO;
"**NCSC**"	shall mean the National Cyber Security Centre or its successor entity (where applicable);
"**Penetration Test**"	shall mean a simulated attack on any Authority Assets, the Authority System (or any part thereof) or the Supplier System (or any part thereof);
"**PCI DSS**"	shall mean the Payment Card Industry Data Security Standard as most recently published by the PCI Security Standards Council, LLC or its successor entity (the "**PCI**");
"**Risk Profile**"	shall mean a description of any set of risks. The set of risks can contain those that relate to a whole organisation, part of an organisation or as otherwise applicable;
"**Security Policies**"	means the policies set out in Annex A;
"**Security Test"**	shall include, but not be limited to, Penetration Test, Vulnerability Scan, Availability Test and any other security related test and audit;
"**Security Standards**"	means the standards set out in Annex B;

"**Tigerscheme**"	shall mean a scheme for authorised penetration tests which scheme is managed by USW Commercial Services Ltd; and
"**Vulnerability Scan**"	shall mean an ongoing activity to identify any potential vulnerability in any Authority Assets, the Authority System (or any part thereof) or the Supplier System (or any part thereof).

1.2 Reference to any notice to be provided by the Supplier to the Authority shall be construed as a notice to be provided by the Supplier to the Authority's Representative.

1.3 The content of this Schedule 5, together with any such additional security requirements set out in Schedule 2 (*Services Description*) shall constitute the "**Security Requirements**".

2. PRINCIPLES OF SECURITY

2.1 The Supplier acknowledges that the Authority places great emphasis on the confidentiality, integrity and availability of the Authority Data and, consequently on the security of:

2.1.1 the Sites;

2.1.2 the IT Environment;

2.1.3 the Information Management System; and

2.1.4 the Services.

2.2 The Supplier acknowledges and agrees that Authority relies upon the Supplier providing all accurate, adequate, and appropriate information in respect of the Services. Where the Supplier considers information relevant to the security of the Services it shall promptly notify the Authority of such information. Notwithstanding the involvement of the Authority in assessing the arrangements which the Supplier implements to ensure the security of the Authority Data and the Information Management System, the Supplier is and shall remain liable for:

2.2.1 the security, confidentiality, integrity and availability of the Authority Data whilst that Authority Data is under the control of the Supplier or any of its Sub-contractors; and

2.2.2 the security of the Information Management System.

2.3 The Supplier shall:

2.3.1 comply with the Security Requirements;

2.3.2 ensure that each Sub-contractor that Processes Authority Data complies with the applicable Security Requirements as notified to the Supplier by the Authority from time to time; and

2.3.3 provide a level of security which is in accordance with the Security Policies and Security Standards, Good Security Practice and Law.

2.4 The Supplier shall provide the Authority with access to Supplier Personnel responsible for information assurance to facilitate the Authority's assessment of the Supplier's compliance with its obligations set out in this Schedule at reasonable times on ten (10) Working Days' written notice.

2.5 The Supplier shall:

2.5.1 monitor the delivery of assurance activities;

2.5.2 monitor security risk impacting upon the operation of the Service;

2.5.3 report Breaches of Security in accordance with the Security Incident Management standard as set out in Annex B;

2.5.4 agree with the Authority the frequency and nature of the security reports to be prepared and submitted by the Supplier to the Authority within twenty (20) Working Days of the Effective Date; and

2.5.5 provide training on a continuing basis for all Supplier Personnel employed or engaged in the provision of the Services in compliance with the Security Policies and Standards.

3. ISO/IEC 27001 COMPLIANCE, CERTIFICATION AND AUDIT

3.1 The Supplier shall, and shall procure that any Sub-contractor (as applicable) shall, obtain and maintain certification to ISO/IEC 27001 (the "**ISO Certificate**") in relation to the Services during the Term. The ISO Certificate shall be provided by the Supplier to the Authority on the dates as agreed by the Parties.

3.2 The Supplier shall appoint:

3.2.1 an Information Security Manager; and

3.2.2 a deputy Information Security Manager who shall have the appropriate experience, authority and expertise to deputise for the Information Security Manager when s/he is on leave or unavailable for any period of time.

3.3 The Supplier shall notify the Authority of the identity of the Information Security Manager on the Commencement Date and, where applicable, within five (5) Working Days following any change in the identity of the Information Security Manager.

3.4 The Supplier shall ensure that it operates and maintains the ISMS during the Term and that the ISMS meets the Security Policies and Security Standards, Good Security Practice and Law and includes:

3.4.1 a scope statement (which covers all of the Services provided under this Contract);

3.4.2 a risk assessment (which shall include any risks specific to the Services);

3.4.3 a statement of applicability;

3.4.4 a risk treatment plan; and

3.4.5 an incident management plan,

in each case as specified by ISO/IEC 27001.

3.5 The Supplier shall provide the ISMS to the Authority upon request within ten (10) Working Days from such request.

3.6 The Supplier shall notify the Authority of any failure to obtain an ISO Certificate or a revocation of an ISO Certificate within two (2) Working Days of confirmation of such failure or revocation. The Supplier shall, at its own expense, undertake those actions required in order to obtain an ISO Certificate following such failure or revocation and provide such ISO Certificate within one (1) calendar month of the initial notification of failure or revocation to the Authority or on a date agreed by the Parties. For the avoidance of doubt, any failure to obtain and/or maintain an ISO Certificate during the Term after the first date on which the Supplier was required to provide the ISO Certificate in accordance with Paragraph 3.1 (regardless of whether such failure is capable of remedy) shall constitute a material Default which is irremediable, entitling the Authority to terminate the Contract in accordance with Clause 31.1.2.

3.7 The Supplier shall carry out regular Security Tests in compliance with ISO/IEC 27001 and shall within ten (10) Working Days after completion of the relevant audit provide any associated security audit reports to the Authority.

3.8 Notwithstanding the provisions of Paragraph 3.1 to Paragraph 3.5, the Authority may, in its absolute discretion, notify the Supplier that it is not in compliance with the Authority's Security Requirements and provide details of such non-compliance. The Supplier shall, at its own expense, undertake those actions required in order to comply with the Authority's Security Requirements within one calendar month following such notification or on a date as agreed by the Parties. For the avoidance of doubt, any failure to comply with the Authority's Security Requirements within the required timeframe (regardless of whether such failure is capable of remedy) shall constitute a material Default which is irremediable, entitling the Authority to terminate the Contract in accordance with Clause 31.1.2.

4. CYBER ESSENTIALS PLUS SCHEME

4.1 The Supplier shall, and shall procure that any Sub-contractor (as applicable) shall, obtain and maintain certification to Cyber Essentials Plus (the "Cyber Essentials Plus Certificate") in relation to the Services during Contract Period. The Cyber Essentials Plus Certificate shall be provided by the Supplier to the Authority annually on the dates as agreed by the Parties.

4.2 The Supplier shall notify the Authority of any failure to obtain, or the revocation of, a Cyber Essentials Plus Certificate within two (2) Working Days of confirmation of such failure or revocation. The Supplier shall, at its own expense, undertake those actions required in order to obtain a Cyber Essentials Plus Certificate following such failure or revocation. For the avoidance of doubt, any failure to obtain and/or maintain a Cyber Essentials Plus Certificate during the Term after the first date on which the Supplier was required to provide a Cyber Essentials Plus Certificate in accordance with Paragraph 4.1 (regardless of whether such failure is capable of remedy) shall constitute a material Default which is irremediable, entitling the Authority to terminate the Contract in accordance with Clause 31.1.2.

4.3 In the event that the Supplier ceases to be compliant with the requirements of this Schedule 5, the Authority may at its absolute discretion direct the Supplier to:

4.3.1 cease using the Authority Data; and/or

4.3.2 promptly return, destroy, and/or erase the Authority Data in accordance with the Security Requirements; and/or

4.3.3 collaborate and/or follow the reasonable instructions of the Authority in respect of achieving compliance with the Security Requirements,

(together the "**Non-Compliance Instructions**") and the Supplier shall and/or shall procure that the relevant Sub-contractor shall promptly comply with such Non-Compliance Instructions.

5. RISK MANAGEMENT

5.1 The Supplier shall create, operate, and maintain policies and processes for risk management (the **Risk Management Policy**) during the Term. Such Risk Management Policy shall include standards and processes for the assessment of any potential risks in relation to the Services and processes to ensure that the Authority's Security Requirements are met (the **Risk Assessment**). The Supplier shall provide the Risk Management Policy to the Authority upon request within ten (10) Working Days of such request. The Authority may, at its absolute discretion, require the Supplier to make changes to the Risk Management Policy to comply with the Authority's Security Requirements. The Supplier shall, at its own expense, promptly undertake those actions required to implement the changes to the Risk Management Policy required by the Authority and to effect such changes in its delivery of

the Services (and in any event within one (1) calendar month of such request or on such other date as agreed by the Parties).

5.2 The Supplier shall carry out a Risk Assessment (i) at least annually, (ii) in the event of a material change in the Supplier System or in the threat landscape or (iii) at the request of the Authority. The Supplier shall provide the report of the Risk Assessment to the Authority, in the case of at least annual Risk Assessments, within five (5) Working Days of completion of the Risk Assessment or, in the case of all other Risk Assessments, within one (1) calendar month after completion of the Risk Assessment or on a date as agreed by the Parties. The Supplier shall notify the Authority within five (5) Working Days if the Risk Profile in relation to the Services has changed materially, for example, but not limited to, from one risk rating to another risk rating.

5.3 If the Authority decides, at its absolute discretion, that any Risk Assessment does not meet the Authority's Security Requirements, the Supplier shall repeat the Risk Assessment within one (1) calendar month of such request or as agreed by the Parties.

5.4 The Supplier shall, and shall procure that any Sub-contractor (as applicable) shall, co-operate with the Authority in relation to the Authority's own risk management processes regarding the Services.

5.5 For the avoidance of doubt, the Supplier shall pay all costs in relation to undertaking any action required to meet the requirements stipulated in this Paragraph 5. Any failure by the Supplier to comply with any requirement of this Paragraph 5 (regardless of whether such failure is capable of remedy), shall constitute a Material Breach which is irremediable, entitling the Authority to terminate the Contract in accordance with Clause 31.1.2.

5.6 The Supplier shall promptly notify the Authority (and in any event, within two (2) Working Days or such other timescale as stipulated in the Security Standards and Security Policies) after becoming aware of:

5.6.1 a significant change to the components or architecture of the Information Management System and/or the ISMS;

5.6.2 a new risk to the components or architecture of the Information Management System and/or the ISMS;

5.6.3 a vulnerability to the components or architecture of the Service;

5.6.4 a change in the threat profile;

5.6.5 a significant change to any risk component;

5.6.6 a significant change in the quantity of Personal Data held within the Service;

5.6.7 a proposal to change any of the Sites from which any part of the Services are provided; and/or

5.6.8 an ISO27001 audit report produced in connection with the Certification Requirements indicating significant concerns.

5.7 Where the Supplier is required to implement a change, including any change to the ISMS, the Supplier shall effect such change at its own cost and expense.

6. SECURITY AUDIT AND ASSURANCE

6.1 The Supplier must ensure that its Implementation Plan aligns with its Information Security Questionnaire response and sets out in sufficient detail how it will ensure compliance with the requirements of this Schedule, including any requirements imposed on Sub-contractors, from the first Operational Services Commencement Date.

6.2 The Supplier shall, and shall procure that any Sub-Contractor (as applicable) shall, complete the information security questionnaire in the format stipulated by the Authority (the "**Information Security Questionnaire**") at least annually. The Supplier shall provide the completed Information Security Questionnaire to the Authority within one calendar month from the date of request.

6.3 The Supplier must report any suspected Breach of Security to the Authority in accordance with Security Requirements, incident management plan and the Security Policies and Security Standards.

6.4 The Authority may, at its sole discretion, prevent the Supplier from using the Information Management System to Process Authority Data if:

6.4.1 the Supplier has not completed the Information Security Questionnaire prior to the Effective Date and/or in accordance with Paragraph 6.2 above; or

6.4.2 the Supplier has completed the Information Security Questionnaire but has failed to evidence (in the Authority's opinion) that it does, and/or will in its performance of the Services, meet the Security Requirements,

until such time that the Supplier has committed in writing to any rectification processes the Authority deems necessary (at the Authority's absolute discretion), and, if required by the Authority, implemented such rectification processes. The exercise of the Authority of its rights under this Paragraph 6.4 shall not constitute an Authority Cause and shall not relieve the Supplier of its liability for Delay Payments which accrue.

6.5 The Supplier shall conduct Security Tests to assess the Information Security of the Supplier System and, if requested, the Authority System. In relation to such Security Tests, the Supplier shall appoint a third party which i) in respect

of any Penetration Test, is duly accredited by CHECK, CREST (International), or Tigerscheme and, ii) in respect of any Security Test to which PCI DSS apply, is an approved scanning vendor duly accredited by the PCI. Such Security Tests shall be carried out:

6.5.1 at least annually;

6.5.2 with no critical or high outstanding issues prior to being introduced into live operations;

6.5.3 in the event of a material change in the Supplier System or in the Authority's System Environment; and

6.5.4 at the request of the Authority which request may include, but is not limited to, a repeat of a previous Security Test, and

the content, and format of any report of such Security Tests shall be approved in advance of the Security Test by the Authority.

6.6 The Supplier shall promptly provide a report of such Security Tests within one (1) calendar month (or within such other timeframe as directed by the Authority) following the completion of such Security Test. The Supplier shall, at its own expense, undertake those actions required to rectify any risks identified by any Security Test in the manner and within the timeframe required by the Authority in its absolute discretion.

6.7 The Authority shall be entitled to send the Authority's Representative to witness the conduct of any Security Test. The Supplier shall provide to the Authority notice of any Security Test at least one (1) month prior to the relevant Security Test.

6.8 The Supplier shall ensure that any testing which could adversely affect the Supplier System shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such tests shall be agreed in advance with the Authority.

6.9 Where the Supplier provides code development services to the Authority, the Supplier shall comply with the Authority's Security Requirements in respect of code development within the Supplier System and the Authority System.

6.10 Where the Supplier provides software development services, the Supplier shall comply with the code development practices specified in the Specification or in the Authority's Security Requirements.

6.11 The Authority, or an agent appointed by it, may undertake Security Tests in respect of the Supplier System, and from time to time may require the Supplier to undertake further Security Tests, after providing advance notice to the Supplier. If any Security Test identifies any non-compliance with the Authority's Security Requirements, the Supplier shall, at its own expense and in accordance with the Security Standards and the Policies, undertake those

actions required in order to rectify such identified non-compliance in the manner and timeframe as stipulated by the Authority at its absolute discretion. The Supplier shall provide all such co-operation and assistance in relation to any Security Test conducted by the Authority as the Authority may reasonably require.

6.12 The Supplier shall notify the Authority immediately if it fails to, or believes that it will not, mitigate an identified vulnerability within the timescales set out in the Security Policies and Security Standards, or as otherwise agreed with, or directed by, the Authority.

6.13 The Authority shall schedule regular security governance review meetings which the Supplier shall, and shall procure that any Sub-contractor (as applicable) shall, attend.

7. PCI DSS COMPLIANCE AND CERTIFICATION

7.1 Where the Supplier obtains, stores, processes or transmits payment card data, the Supplier shall comply with the PCI DSS.

7.2 The Supplier shall obtain and maintain up-to-date attestation of compliance certificates ("**AoC**") provided by a qualified security assessor accredited by the PCI and up-to-date reports on compliance ("**RoC**") provided by a qualified security assessor or an internal security assessor, in each case accredited by the PCI (each with the content and format as stipulated by the PCI and such reports the **"PCI Reports"**), during the Term. The Supplier shall provide the respective PCI Reports to the Authority upon request within ten (10) Working Days of such request.

7.3 The Supplier shall notify the Authority of any failure to obtain a PCI Report or a revocation of a PCI Report within two (2) Working Days of confirmation of such failure or revocation. The Supplier shall, at its own expense, undertake those actions required in order to obtain a PCI Report following such failure or revocation within one calendar month of such failure or revocation.

8. SECURITY POLICIES AND SECURITY STANDARDS

8.1 The Supplier shall, and shall procure that any Sub-contractor (as applicable) shall comply with the Security Policies and Security Standards and shall provide evidence of such compliance to the Authority within one (1) month of request.

8.2 Notwithstanding the foregoing, the Authority's Security Requirements applicable to the Services may be subject to change following certain events including, but not limited to, any relevant change in the delivery of the Services. Where any such change constitutes a Contract Change, any change in the Authority's Security Requirements resulting from such Contract Change (if any) shall be agreed by the Parties in accordance with the Contract Change Procedure. Where any such change constitutes an Operational Change, any change in the Authority's Security Requirements resulting from such

Operational Change (if any) shall be agreed by the Parties and documented in the relevant Operational Change Confirmation.

8.3 The Supplier shall, and shall procure that any Sub-contractor (as applicable) shall, maintain appropriate records and is otherwise able to demonstrate compliance with the Security Policies and Security Standards.

9. CYBER SECURITY INFORMATION SHARING PARTNERSHIP

9.1 The Supplier may require a nominated representative of the Supplier to join the Cyber Security Information Sharing Partnership on behalf of the Supplier during the Term, in which case the Supplier's nominated representative shall participate in the Cyber Security Information Sharing Partnership for the exchange of cyber threat information.

9.2 If the Supplier elects a nominated representative to join the Cyber Security Information Sharing Partnership in accordance with Paragraph 9.1 above, it shall review the NCSC weekly threat reports on a weekly basis and implement recommendations in line with the Supplier's Risk Management Policy.

ANNEX A – AUTHORITY SECURITY POLICIES

The Security Policies are published on: https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards unless specified otherwise:

Acceptable Use Policy

Information Security Policy

Physical Security Policy

Information Management Policy

Email Policy

Technical Vulnerability Management Policy

Remote Working Security Policy

Social Media Policy

Forensic Readiness Policy

SMS Text Policy

Privileged Users Security Policy

User Access Control Policy

Security Classification Policy

Cryptographic Key Management Policy

HMG Personnel Security Controls – May 2018
(published on https://www.gov.uk/government/publications/hmg-personnel-security-controls)

NCSC Secure Sanitisation of Storage Media (published on https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media)

ANNEX B – SECURITY STANDARDS

The Security Standards are published on:

https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards:

SS-001 - Part 1 - Access & Authentication Controls
SS-001 - Part 2 - Privileged User Access Controls
SS-002 – Public Key Infrastructure & Key Management
SS-003 - Software Development
SS-005 - Database Management System
SS-006 - Security Boundaries
SS-007 - Use of Cryptography
SS-008 - Server Operating System
SS-009 - Hypervisor
SS-010 - Desktop Operating System
SS-011 - Containerisation
SS-012 - Protective Monitoring Standard for External Use
SS-013 - Firewall Security
SS-014 - Security Incident Management
SS-015 - Malware Protection
SS-016 - Remote Access
SS-017 - Mobile Device
SS-018 - Network Security Design
SS-019 - Wireless Network
SS-022 - Voice & Video Communications
SS-023 - Cloud Computing
SS-025 - Virtualisation
SS-027 - Application Security Testing
SS-028 - Microservices Architecture
SS-029 - Securely Serving Web Content
SS-030 - Oracle Database Security
SS-031 - Domain Management
SS-033 – Security Patching