Call-Off Schedule 9 – Minimum Security Requirements

GENERAL

The Supplier shall, and shall procure that any Subcontractor (as applicable) shall, comply with the Buyer's security requirements as set out in the Contract which include the requirements set out in this Call-Off Schedule 9 (the "**Buyer's Security Requirements**"). The Buyer's Security Requirements include, but are not limited to, requirements regarding the confidentiality, integrity and availability of Buyer Assets, the Buyer's Operating Environment and the Supplier's System environment.

Terms used in this Schedule 9 which are not defined below shall have the meanings given to them in Joint Schedule 1 (Definitions).

1. Definitions

1.1 In this Schedule 9, the following definitions shall apply:

"Buyer Personnel"	shall mean all persons employed by the Buyer including directors, officers, employees together with the Buyer's servants, agents, consultants, contractors and suppliers but excluding the Supplier and any Subcontractor (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 Buyer.
"**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**"	shall mean the Government-backed, industry-supported scheme managed by the NCSC 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; and c) the Government's security policies, frameworks, standards and guidelines relating to Information Security.
"**Information Security**"	shall mean: a) the protection and preservation of: i) the confidentiality, integrity and availability of any Buyer Assets, the Buyer's Systems Environment (or any part thereof) and the Supplier's Systems Environment (or any part thereof); ii) related properties of information including, but not limited to, authenticity, accountability, and non-repudiation; and b) compliance with all Law applicable to the processing, transmission, storage and disposal of Buyer 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 Buyer's Security Requirements.

"**Information Security Management System ("ISMS")**"	shall mean the set of policies, processes and systems designed, implemented and maintained by the Supplier to manage Information Security Risk as specified by ISO/IEC 27001.
"**Information Security Questionnaire**"	shall mean the Buyer's set of questions used to audit and on an ongoing basis assure the Supplier's compliance with the Buyer'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 Buyer Assets, the Buyer's Systems Environment (or any part thereof) or the Supplier's Systems Environment (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 risk. The set of risks can contain those that relate to a whole organisation, part of an organisation or as otherwise applicable.

"**Security Test"**	shall include, but not be limited to, Penetration Test, Vulnerability Scan, Availability Test and any other security related test and audit.
"**Tigerscheme**"	shall mean a scheme for authorised penetration tests which scheme is managed by the University of Wales.
"**Vulnerability Scan**"	shall mean an ongoing activity to identify any potential vulnerability in any Buyer Assets, the Buyer's Systems Environment (or any part thereof) or the Supplier's Systems Environment (or any part thereof).

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

2. Principles Of Security

2.1 The Supplier shall at all times comply with the Buyer's Security Requirements and provide a level of security which is in accordance with the Security Policies and Standards, Good Security Practice and Law.

3. Iso/Iec 27001 Compliance And Audit

3.1 The Supplier shall, and shall procure that any Subcontractor (as applicable) shall, comply with ISO/IEC 27001 in relation to the Services during the Contract Period.

3.2 The Supplier shall appoint an Information Security Manager and shall notify the Buyer of the identity of the Information Security Manager on the Start Date and, where applicable, within five (5) Working Days following any change in the identity of the Information Security Manager.

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

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

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

3.1.3 a statement of applicability;

3.1.4 a risk treatment plan; and

3.1.5 an incident management plan

in each case as specified by ISO/IEC 27001.

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

3.4 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 Buyer.

3.5 Notwithstanding the provisions of paragraph 3.1 to paragraph 3.4, the Buyer may, in its absolute discretion, notify the Supplier that it is not in compliance with the Buyer'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 Buyer's Security Requirements within one (1) Month following such notification or on a date as agreed by the Parties. For the avoidance of doubt, any failure to comply with the Buyer's Security Requirements within the required timeframe (regardless of whether such failure is capable of remedy) shall constitute a material Default entitling the Buyer to exercise its rights under Clause 21 (*Termination*) of the Special Terms.

4. Cyber Essentials Scheme

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

4.2 The Supplier shall notify the Buyer of any failure to obtain, or the revocation of, a Cyber Essentials 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 Certificate following such failure or revocation. For the avoidance of doubt, any failure to obtain and/or maintain a Cyber Essentials Certificate during the Contract Period after the first date on which the Supplier was required to provide a Cyber Essentials Certificate in accordance with paragraph 4.1 (regardless of whether such failure is capable of remedy) shall constitute a material Default entitling the Buyer to exercise its rights under Clause 21 (*Termination*) of the Special Terms.

5. Risk Management

5.1 The Supplier shall operate and maintain policies and processes for risk management (the "**Risk Management Policy**") during the Contract Period which includes standards and processes for the assessment of any potential risks in relation to the Services and processes to ensure that the Buyer's Security Requirements are met (the "**Risk Assessment**"). The Supplier shall provide the Risk Management Policy to the Buyer upon request within ten (10) Working Days of such request. The Buyer may, at its absolute discretion, require changes to the Risk Management Policy to comply with the Buyer's Security Requirements. The Supplier shall, at its own expense, undertake those

actions required in order to implement the changes required by the Buyer within one (1) Month of such request or on a 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's Systems Environment or in the threat landscape or (iii) at the request of the Buyer. The Supplier shall provide the report of the Risk Assessment to the Buyer, 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) Month after completion of the Risk Assessment or on a date as agreed by the Parties. The Supplier shall notify the Buyer 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 Buyer decides, at its absolute discretion, that any Risk Assessment does not meet the Buyer's Security Requirements, the Supplier shall repeat the Risk Assessment within one (1) 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 Buyer in relation to the Buyer'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 Default entitling the Buyer to exercise its rights under clause 21 (*Termination*) of the Special Terms.

6. Security Audit And Assurance

6.1 The Supplier shall, and shall procure that any Subcontractor (as applicable) shall, complete the information security questionnaire in the format stipulated by the Buyer (the "**Information Security Questionnaire**") at least annually or at the request by the Buyer. The Supplier shall provide the completed Information Security Questionnaire to the Buyer within one (1) Month from the date of request.

6.2 The Supplier shall conduct Security Tests to assess the Information Security of the Supplier's Systems Environment and, if requested, the Buyer's Systems Environment. 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 Test shall be carried out (i) at least annually, (ii) in the event of a material change in the Supplier's Systems Environment or in the Buyer's System Environment or (iii) at the request of the Buyer which request may include, but is not limited to, a repeat of a previous Security Test. The content, and format of any report of such Security Tests shall be approved in advance of the Security Test by the Buyer. The Supplier shall

provide any report of such Security Tests within one (1) Month following the completion of such Security Test or on a date agreed by the Parties. 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 Buyer in its absolute discretion.

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

6.4 Where the Supplier provides code development services to the Buyer, the Supplier shall comply with the Buyer's Security Requirements in respect of code development within the Supplier's Systems Environment and the Buyer's Systems Environment.

6.5 Where the Supplier provides software development services, the Supplier shall comply with the code development practices specified in the specification or in the Buyer's Security Requirements.

6.6 The Buyer, or an agent appointed by it, may undertake Security Tests in respect of the Supplier's Systems Environment after providing advance notice to the Supplier. If any Security Test identifies any non-compliance with the Buyer's Security Requirements, the Supplier shall, at its own expense, undertake those actions required in order to rectify such identified non-compliance in the manner and timeframe as stipulated by the Buyer at its absolute discretion. The Supplier shall provide all such co-operation and assistance in relation to any Security Test conducted by the Buyer as the Buyer may reasonably require.

6.7 The Buyer shall schedule regular security governance review meetings which the Supplier shall, and shall procure that any Subcontractor (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 self-assessment questionnaires ("**SAQ**") completed 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 Contract Period. The Supplier shall provide the respective PCI Reports to the Buyer upon request within ten (10) Working Days of such request.

7.3 The Supplier shall notify the Buyer 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 (1) Month of such failure or revocation.

8. Security Policies And Standards

8.1 The Supplier shall, and shall procure that any Subcontractor (as applicable) shall, comply with the Security Policies and Standards set out ANNEX A and ANNEX B.

8.2 Notwithstanding the foregoing, the Buyer'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 Variation, any change in the Buyer's Security Requirements resulting from such Variation (if any) shall be agreed by the Parties in accordance with the Variation Procedure. Where any such change constitutes an operational variation, any change in the Buyer's Security Requirements resulting from such operational variation (if any) shall be agreed by the Parties and documented in the relevant Variation Authorisation Note.

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

9. Cyber Security Information Sharing Partnership

9.1 The Supplier may become a member of the Cyber Security Information Sharing Partnership in accordance with the recommendations by the NCSC during the Contract Period. The Supplier may participate in the Cyber Security Information Sharing Partnership for the exchange of cyber threat information.

9.2 Where the Supplier becomes a member of the Cyber Security Information Sharing Partnership, 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 – BUYER SECURITY POLICIES AND STANDARDS

The Security Policies are published on:

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

a) Acceptable Use Policy
b) Information Security Policy
c) Physical Security Policy
d) Information Management Policy
e) Email Policy
f) Technical Vulnerability Management Policy
g) Remote Working Policy
h) Social Media Policy
i) Forensic Readiness Policy
j) SMS Text Policy
k) Privileged Users Security Policy
l) User Access Control Policy
m) Security Classification Policy
n) Cryptographic Key Management Policy
o) HMG Personnel Security Controls – May 2018 (published on https://www.gov.uk/government/publications/hmg-personnel-security-controls)
p) 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:

a) SS-001 - Part 1 - Access & Authentication Controls
b) SS-001 - Part 2 - Privileged User Access Controls
c) SS-002 - PKI & Key Management
d) SS-003 - Software Development
e) SS-005 - Database Management System Security Standard
f) SS-006 - Security Boundaries
g) SS-007 - Use of Cryptography
h) SS-008 - Server Operating System
i) SS-009 - Hypervisor
j) SS-010 - Desktop Operating System
k) SS-011 - Containerisation
l) SS-012 - Protective Monitoring Standard for External Use
m) SS-013 - Firewall Security
n) SS-014 - Security Incident Management
o) SS-015 - Malware Protection
p) SS-016 - Remote Access
q) SS-017 - Mobile Devices
r) SS-018 - Network Security Design
s) SS-019 - Wireless Network
t) SS-022 - Voice & Video Communications
u) SS-023 - Cloud Computing
v) SS-025 - Virtualisation
w) SS-027 - Application Security Testing
x) SS-028 - Microservices Architecture
y) SS-029 - Securely Serving Web Content
z) SS-030 - Oracle Database
aa) SS-031 - Domain Management
bb) SS-033 - Patching