



Crown  
Commercial  
Service

## Digital Outcomes and Specialists 5 (RM1043.7)

### Special Terms

DWP UC User Research Recruitment Services

#### Special Term 1

**ANNEX A - AUTHORITY SECURITY POLICIES AND STANDARDS**

**ANNEX B - SECURITY STANDARDS**

#### Special Term 1

#### **SCHEDULE 9 – SECURITY REQUIREMENTS LEVEL 3 AND 4**

##### **GENERAL**

The Contractor 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 9 to the Contract (the "**Authority's Security Requirements**"). The Authority's Security Requirements include, but are not limited to, requirements regarding the confidentiality, integrity and availability of Authority Assets, the Authority's Systems Environment and the Contractor's Systems Environment.

Terms used in this Schedule 9 which are not defined below shall have the meanings given to them in clause A1 (Definitions and Interpretations) of the Contract.

#### **1. DEFINITIONS**

1.1 In this Schedule 9, 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 Contractor and any Sub-contractor (as applicable).
<b>“Availability Test”</b>	shall mean the activities performed by the Contractor to confirm the availability of any or all components of any relevant ICT system as specified by the Authority.
<b>“CHECK”</b>	shall mean the scheme for authorised penetration tests which scheme is managed by the NCSC.
<b>“Cloud”</b>	shall mean an off-premise network of remote ICT servers on the Internet to store, process, manage and transmit data.
<b>“Cyber Essentials”</b>	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.
<b>“Cyber Security Information Sharing Partnership” or “CiSP”</b>	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.
<b>“Good Security Practice”</b>	<p>shall mean:</p> <ul style="list-style-type: none"> <li>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);</li> <li>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</li> </ul>

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 Authority Assets, the Authority's Systems Environment (or any part thereof) and the Contractor'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 Authority Assets.

**"Information Security Manager"** shall mean the person appointed by the Contractor with the appropriate experience, authority and expertise to ensure that the Contractor complies with the Authority's Security Requirements.

**"Information Security Management System ("ISMS")"** shall mean the set of policies, processes and systems designed, implemented and maintained by the Contractor 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 Contractor'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’s Systems Environment (or any part thereof) or the Contractor’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 USW Commercial Services Ltd.

**“Vulnerability Scan”**

shall mean an ongoing activity to identify any potential vulnerability in any Authority Assets, the Authority’s Systems Environment (or any part thereof) or the Contractor’s Systems Environment (or any part thereof).

- 1.2 Reference to any notice to be provided by the Contractor to the Authority shall be construed as a notice to be provided by the Contractor to the Authority’s Representative.

## **2. PRINCIPLES OF SECURITY**

- 2.1 The Contractor shall at all times comply with the Authority'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 Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, comply with ISO/IEC 27001 in relation to the Services during the Contract Period.
- 3.2 The Contractor shall appoint an Information Security Manager and shall notify the Authority of the identity of the Information Security Manager on the Commencement Date and, where applicable, within 5 Working Days following any change in the identity of the Information Security Manager.
- 3.3 The Contractor shall ensure that it operates and maintains the Information Security Management System during the Contract Period and that the Information Security Management System meets the Security Policies and Standards, Good Security Practice and Law and includes:

- a) a scope statement (which covers all of the Services provided under this Contract);
  - b) a risk assessment (which shall include any risks specific to the Services);
  - c) a statement of applicability;
  - d) a risk treatment plan; and
  - e) an incident management plan
- in each case as specified by ISO/IEC 27001.

The Contractor shall provide the Information Security Management System to the Authority upon request within 10 Working Days from such request.

- 3.4 The Contractor shall carry out regular Security Tests in compliance with ISO/IEC 27001 and shall within 10 Working Days after completion of the relevant audit provide any associated security audit reports to the Authority.
- 3.5 Notwithstanding the provisions of paragraph 3.1 to paragraph 3.4, the Authority may, in its absolute discretion, notify the Contractor that it is not in compliance with the Authority's Security Requirements and provide details of such non-compliance. The Contractor 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 Breach entitling the Authority to exercise its rights under Clause 10.4.1(d) of the Core Terms.

#### 4. CYBER ESSENTIALS SCHEME

- 4.1 The Contractor shall, and shall procure that any Sub-contractor (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 Contractor to the Authority annually on the dates as agreed by the Parties.
- 4.2 The Contractor shall notify the Authority of any failure to obtain, or the revocation of, a Cyber Essentials Certificate within 2 Working Days of confirmation of such failure or revocation. The Contractor 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 Contractor 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 Breach entitling the Authority to exercise its rights under Clause 10.4.1(d) of the Core Terms.

#### 5. RISK MANAGEMENT

- 5.1 The Contractor 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 Authority's Security Requirements are met (the **Risk Assessment**). The Contractor shall provide the Risk Management Policy to the Authority upon request within 10 Working Days of such request. The Authority may, at its absolute discretion, require changes to the Risk Management Policy to comply with the Authority's Security Requirements. The Contractor shall, at its own expense, undertake those actions required in order to implement the changes required by the Authority within one calendar month of such request or on a date as agreed by the Parties.
- 5.2 The Contractor shall carry out a Risk Assessment (i) at least annually, (ii) in the event of a material change in the Contractor's Systems Environment or in the threat landscape or (iii) at the request of the Authority. The Contractor shall provide the report of the Risk Assessment to the Authority, in the case of at least annual Risk Assessments, within 5 Working Days of completion of the Risk Assessment or, in the case of all other Risk Assessments, within one calendar month after completion of the Risk Assessment or on a date as agreed by the Parties. The Contractor shall notify the Authority within 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 Contractor shall repeat the Risk Assessment within one calendar month of such request or as agreed by the Parties.

- 5.4 The Contractor 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 Contractor shall pay all costs in relation to undertaking any action required to meet the requirements stipulated in this paragraph 5. Any failure by the Contractor to comply with any requirement of this paragraph 5 (regardless of whether such failure is capable of remedy), shall constitute a Material Breach entitling the Authority to exercise its rights under Clause 10.4.1(d) of the Core Terms.

## 6. SECURITY AUDIT AND ASSURANCE

- 6.1 The Contractor 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 or at the request by the Authority. The Contractor shall provide the completed Information Security Questionnaire to the Authority within one calendar month from the date of request.
- 6.2 The Contractor shall conduct Security Tests to assess the Information Security of the Contractor's Systems Environment and, if requested, the Authority's Systems Environment. In relation to such Security Tests, the Contractor 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 Contractor's Systems Environment or in the Authority's System Environment or (iii) at the request of the Authority 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 Authority. The Contractor shall provide any report of such Security Tests within one calendar month following the completion of such Security Test or on a date agreed by the Parties. The Contractor 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.
- 6.3 The Authority shall be entitled to send the Authority's Representative to witness the conduct of any Security Test. The Contractor shall provide to the Authority notice of any Security Test at least one month prior to the relevant Security Test.
- 6.4 The Authority, or an agent appointed by it, may undertake Security Tests in respect of the Contractor's Systems Environment after providing advance notice to the Contractor. If any Security Test identifies any non-compliance with the Authority's Security Requirements, the Contractor 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 Authority at its absolute discretion. The Contractor shall provide all such co-operation and assistance in relation to any Security Test conducted by the Authority as the Authority may reasonably require.

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

## **7. SECURITY POLICIES AND STANDARDS**

- 7.1 The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, comply with the Security Policies and Standards set out Annex A and B.
- 7.2 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.
- 7.3 The Contractor 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 Standards.

## **8. CYBER SECURITY INFORMATION SHARING PARTNERSHIP**

- 8.1 The Contractor may become a member of the Cyber Security Information Sharing Partnership in accordance with the recommendations by the NCSC during the Contract Period. The Contractor may participate in the Cyber Security Information Sharing Partnership for the exchange of cyber threat information.
- 8.2 Where the Contractor 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 Contractor's Risk Management Policy.



## **Protection on Information**

The Contractor and any of its Sub-contractors, shall not access, process, host or transfer Authority Data outside the United Kingdom without the prior written consent of the Authority, and where the Authority gives consent, the Contractor shall comply with any reasonable instructions notified to it by the Authority in relation to the Authority Data in question. The provisions set out in this paragraph E1.9 shall apply to Landed Resources.

Where the Authority has given its prior written consent to the Contractor to access, process, host or transfer Authority Data from premises outside the United Kingdom (in accordance with clause E1.9 of the Contract):-

- a) the Contractor must notify the Authority (in so far as they are not prohibited by Law) where any Regulatory Bodies seek to gain or has gained access to such Authority Data;
- b) the Contractor shall take all necessary steps in order to prevent any access to, or disclosure of, any Authority Data to any Regulatory Bodies outside the United Kingdom unless required by Law without any applicable exception or exemption.

## **ANNEX A – AUTHORITY 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) Remote Working Policy
- g) Social Media Policy
- h) Forensic Readiness Policy
- i) SMS Text Policy
- j) User Access Control Policy
- k) Security Classification Policy
- l) HMG Personnel Security Controls – May 2018  
(published on <https://www.gov.uk/government/publications/hmg-personnel-security-controls>)
- m) 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-007 - Use of Cryptography
- d) SS-012 - Protective Monitoring Standard for External Use
- e) SS-014 - Security Incident Management