Schedule 6

Security Requirements and Plan

1 Introduction

1.1 This Schedule covers:

(a) principles of security for the Contractor System, derived from the Security Policy, including without limitation principles of physical and information security;

(b) the creation of the Security Plan;

(c) audit and testing of the Security Plan;

(d) conformance to ISO/IEC:27002 (Information Security Code of Practice) and ISO/IEC 27001 (Information Security Requirements Specification) (Standard Specification); and

(e) breaches of security.

2 Principles of Security

2.1 The Contractor acknowledges that the Authority places great emphasis on confidentiality, integrity and availability of information and consequently on the security of the Premises and the security for the Contractor System. The Contractor also acknowledges the confidentiality of the Authority's Data.

2.2 The Contractor shall be responsible for the security of the Contractor System and shall at all times provide a level of security which;

(a) is in accordance with Good Industry Practice and Law;

(b) complies with the Security Policy;

(c) meets any specific security threats to the Contractor System; and

(d) complies with ISO/IEC27002 and ISO/IEC27001 in accordance with paragraph 5 of this Schedule; and

(e) meets the requirements of the Cyber Essentials Scheme, unless deemed out of scope for this requirement.

2.3 Without limiting paragraph 2.2, the Contractor shall at all times ensure that the level of security employed in the provision of the Services is appropriate to minimise the following risks:

(a) loss of integrity of Authority Data;

(b) loss of confidentiality of Authority Data;

(c) unauthorised access to, use of, or interference with Authority Data by any person or organisation;

(d) unauthorised access to network elements and buildings;

(e) use of the Contractor System or Services by any third party in order to gain unauthorised access to any computer resource or Authority Data; and

(f) loss of availability of Authority Data due to any failure or compromise of the Services; [and]

(g) loss of confidentiality, integrity and availability of Authority Data through cyber/internet threats.

3 Security Plan

Introduction

3.1 The Contractor shall develop, implement and maintain a Security Plan to apply during the Contract Period and after the end of the Contract Period in accordance with the Exit Management Strategy, which will be approved by the Authority, tested, periodically updated and audited in accordance with this Schedule.

3.2 A draft Security Plan provided by the Contractor as part of its bid is set out in Appendix B.

Development

3.3 Within twenty (20) Working Days after the Commencement Date and in accordance with paragraphs 3.10 to 3.12 (Amendment and Revision), the Contractor will prepare and deliver to the Authority for approval the full and final Security Plan which will be based on the draft Security Plan set out in Appendix B.

3.4 If the Security Plan is approved by the Authority it will be adopted immediately. If the Security Plan is not approved by the Authority the Contractor shall amend it within ten (10)] Working Days of a notice of non-approval from the Authority and re-submit to the Authority for approval. The Parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Authority. If the Authority does not approve the Security Plan following its resubmission, the matter will be resolved in accordance with clause **Error! Reference source not found.** (Dispute Resolution). No approval to be given by the Authority pursuant to this paragraph 3.4 of this schedule may be unreasonably withheld or delayed. However any failure to approve the Security Plan on the grounds that it does not comply with the requirements set out in paragraphs 3.1 to 3.9 shall be deemed to be reasonable.

Content

3.5 The Security Plan will set out the security measures to be implemented and maintained by the Contractor in relation to all aspects of the Services and all processes associated

with the delivery of the Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Services comply with:

(a) the provisions of this Contract;

(b) this Schedule (including the principles set out in paragraph 2);

(c) the provisions of Schedule 1 relating to security;

(d) ISO/IEC27002 and ISO/IEC27001; and

(e) the data protection compliance guidance produced by the Authority.

3.6 The references to standards, guidance and policies set out in paragraph 3.5 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, from time to time.

3.7 In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Contractor should notify the Authority's Representative of such inconsistency immediately upon becoming aware of the same, and the Authority's Representative shall, as soon as practicable, advise the Contractor which provision the Contractor shall be required to comply with.

3.8 The Security Plan will be structured in accordance with ISO/IEC27002 and ISO/IEC27001.

3.9 Where the Security Plan references any document which is not in the possession of the Authority, a copy of the document will be made available to the Authority upon request. The Security Plan shall be written in plain English in language which is readily comprehensible to the staff of the Contractor and the Authority engaged in the Services and shall not reference any other documents which are not either in the possession of the Authority or otherwise specified in this Schedule.

Amendment and Revision

3.10 The Security Plan will be fully reviewed and updated by the Contractor annually, or from time to time to reflect:

(a) emerging changes in Good Industry Practice;

(b) any change or proposed change to the Contractor System, the Services and/or associated processes; and

(c) any new perceived or changed threats to the Contractor System; and

(d) a reasonable request by the Authority.

3.11 The Contractor will provide the Authority with the results of such reviews as soon as reasonably practicable after their completion and amend the Security Plan at no additional cost to the Authority.

3.12 Any change or amendment which the Contractor proposes to make to the Security Plan as a result of an Authority request or change to the Schedule 1 or otherwise shall be subject to the change control procedure and shall not be implemented until approved in writing by the Authority.

4 Audit and Testing

4.1 The Contractor shall conduct tests of the processes and countermeasures contained in the Security Plan ("Security Tests") on an annual basis or as otherwise agreed by the Parties. The date, timing, content and conduct of such Security Tests shall be agreed in advance with the Authority.

4.2 The Authority shall be entitled to send a representative to witness the conduct of the Security Tests. The Contractor shall provide the Authority with the results of such tests (in a form approved by the Authority in advance) as soon as practicable after completion of each Security Test.

4.3 Without prejudice to any other right of audit or access granted to the Authority pursuant to this Contract, the Authority shall be entitled at any time and without giving notice to the Contractor to carry out such tests (including penetration tests) as it may deem necessary in relation to the Security Plan and the Contractor's compliance with and implementation of the Security Plan. The Authority may notify the Contractor of the results of such tests after completion of each such test. Security Tests shall be designed and implemented so as to minimise the impact on the delivery Services. If such tests impact adversely on its ability to deliver the Services to the agreed Service Levels, the Contractor shall be granted relief against any resultant under-performance for the period of the tests.

4.4 Where any Security Test carried out pursuant to paragraphs 4.2 or 4.3 above reveals any actual or potential security failure or weaknesses, the Contractor shall promptly notify the Authority of any changes to the Security Plan (and the implementation thereof) which the Contractor proposes to make in order to correct such failure or weakness. Subject to the Authority's approval in accordance with paragraph 3.12, the Contractor shall implement such changes to the Security Plan in accordance with the timetable agreed with the Authority or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the Security Plan to address a non-compliance with the Security Policy or security requirements, the change to the Security Plan shall be at no additional cost to the Authority. For the purposes of this paragraph 4, a weakness means vulnerability in security and a potential security failure means a possible breach of the Security Plan or security requirements.

5 Compliance with ISO/IEC 27001

5.1 If certain parts of the Security Policy do not conform to Good Industry Practice as described in ISO27002 and, as a result, the Contractor reasonably believes that its certification to ISO 27001 would fail in regard to these parts, the Contractor shall promptly notify the Authority of this and the Authority in its absolute discretion may waive the requirement to certification in respect of the relevant parts.

5.2 The Contractor shall carry out such regular security audits as may be required by the British Standards Institute in order to maintain delivery of the Services in compliance

with security aspects of ISO 27001 and shall promptly provide to the Authority any associated security audit reports and shall otherwise notify the Authority of the results of such security audits.

5.3 If it is the Authority's reasonable opinion that compliance with the principles and practices of ISO 27001 is not being achieved by the Contractor, then the Authority shall notify the Contractor of the same and give the Contractor a reasonable time (having regard to the extent of any non-compliance and any other relevant circumstances) to become compliant with the principles and practices of ISO 27001. If the Contractor does not become compliant within the required time then the Authority has the right to obtain an independent audit against these standards in whole or in part.

5.4 If, as a result of any such independent audit as described in paragraph 5.4 the Contractor is found to be non-compliant with the principles and practices of ISO 27001 then the Contractor shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the Authority in obtaining such audit.

6 Breach of Security

6.1 Either party shall notify the other immediately upon becoming aware of any Breach of Security including, but not limited to an actual, potential or attempted breach, or threat to, the Security Plan.

6.2 Upon becoming aware of any of the circumstances referred to in paragraph 6.1, the Contractor shall:

(a) immediately take all reasonable steps necessary to;

(i) remedy such breach or protect the Contractor System against any such potential or attempted breach or threat; and

(ii) prevent an equivalent breach in the future.

Such steps shall include any action or changes reasonably required by the Authority. In the event that such action is taken in response to a breach that is determined by the Authority acting reasonably not to be covered by the obligations of the Contractor under this Contract, then the Contractor shall be entitled to refer the matter to the change control procedure in clause **Error! Reference source not found.** (Variation).

(b) as soon as reasonably practicable provide to the Authority full details (using such reporting mechanism as may be specified by the Authority from time to time) of such actual, potential or attempted breach and of the steps taken in respect thereof.

Appendix A

Security Policy for Contractors

1 The Authority treats its information as a valuable asset and considers that it is essential that information must be protected, together with the systems, equipment and processes which support its use. These information assets may include data, text, drawings, diagrams, images or sounds in electronic, magnetic, optical or tangible media, together with any Personal Data for which the Authority is the Data Controller.

2 In order to protect Authority information appropriately, our contractors must provide the security measures and safeguards appropriate to the nature and use of the information. All Contractors of services to the Authority must comply, and be able to demonstrate compliance, with the Authority's relevant policies and standards.

3 The Chief Executive or other suitable senior official of each contractor must agree in writing to comply with these policies and standards. Each contractor must also appoint a named officer who will act as a first point of contact with the Authority for security issues. In addition, all staff working for the contractor and where relevant sub-contractors, with access to Authority IT systems, services or Authority information must be made aware of these requirements and must comply with them.

4 All contractors must comply with the relevant Authority standards. The standards are based on and follow the same format as ISO27001, but with specific reference to the Authority's use.

5 The following are key requirements and all Contractors must comply with relevant Authority policies concerning:

(a) Personnel Security:

(i) Staff recruitment in accordance with government requirements for pre-employment checks;

(ii) Staff training and awareness of Authority security and any specific contract requirements;

(b) Secure Information Handling and Transfers: physical and electronic handling, processing and transferring of Authority Data, including secure access to systems and the use of encryption where appropriate;

(c) Portable Media: the use of encrypted laptops and encrypted storage devices and other removable media when handling Authority information;

(d) Offshoring: the Authority Data must not be processed outside the United Kingdom without Approval and must at all times comply with the DPA;

(e) Premises Security: security of premises and control of access; and

(f) Security Incidents: includes identification, managing and agreed reporting procedures for actual or suspected security breaches.

6 All contractors must implement appropriate arrangements which ensure that the Authority's information and any other Authority assets are protected in accordance with prevailing statutory and central government requirements. These arrangements will clearly vary according to the size of the organisation.

7 It is the Contractor’s responsibility to monitor compliance of any Sub- contractors and provide assurance to the Authority.

8 Failure to comply with any of these policies or standards could result in termination of current Contract.

Appendix B

Draft Security Plan

REDACTED