Revision Number	Revision Date	Summary of Changes	Changes Made by
0.1	Date of OJEU	Issued at the date of OJEU.	DMO

SCHEDULE 7: SECURITY REQUIREMENTS

[Note to Bidders: The Customer reserves the right to add further security rquirements to this Schedule post OJEU.]

1. INTRODUCTION

1.1 The purpose of this Schedule is to ensure a good organisational approach to security under which the specific requirements of this Contract will be met;

1.2 This Schedule covers:

1.2.1 principles of protective security to be applied in delivering the Services;

1.2.2 the creation and maintenance of the Security Management Plan; and

1.2.3 obligations in the event of actual or attempted Breaches of Security.

2. PRINCIPLES OF SECURITY

2.1 The Supplier acknowledges that the Customer places great emphasis on the reliability of the performance of the Services, confidentiality, integrity and availability of information and consequently on security.

2.2 The Supplier shall be responsible for the effective performance of its security obligations and shall at all times provide a level of security which:

2.2.1 is in accordance with the Law and this Contract;

2.2.2 conforms to and demonstrates security best practices;

2.2.3 complies with the Security Policy;

2.2.4 meets any specific security threats of immediate relevance to the Services and/or the Customer Data;

2.2.5 complies with the Customer's ICT Policy;

2.2.6 features "security by design";

2.2.7 prioritises the confidentiality, integrity and availability of the Solution and Customer Data;

2.2.8 takes confidentiality of Customer Data and the Customer's business seriously during the Implementation and subsequent Service delivery phases;

2.2.9 protects the Customer's reputation at all times; and

2.2.10 ensures Supplier Personnel adhere to the Customer's security policies and requirements when at the Customer Premises.

2.3 Subject to Clause 34 of this Contract (Security and Protection of Information) the references to standards, guidance and policies contained or set out in paragraph 2.2 of this Schedule 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, as notified to the Supplier from time to time.

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

3. SECURITY MANAGEMENT PLAN

3.1 At the Commencement Date the Customer has Approved a security management plan prepared by the Supplier in connection with the Services, such Approved Security Management Plan shall be adopted by the Supplier immediately and incorporated into this Contract at Annex 2 (Security Management Plan) and thereafter operated and maintained in accordance with this Schedule.

3.2 During the Contract Period (and after the end of the Contract Period if so directed by the Customer), the Supplier shall:

3.2.1 implement, maintain and comply with the Security Management Plan; and

3.2.2 test, update and audit the Security Management Plan in accordance with this Schedule.

3.3 The Supplier shall comply with the provisions of the Security Management Plan at its own cost.

3.4 Approval by the Customer of the security management plan or any change to the Security Management Plan shall not relieve the Supplier of its obligations under this Schedule.

3.5 Content of the Security Management Plan

3.5.1 The Security Management Plan shall:

(a) comply with the principles of security set out in paragraph 2 of this Schedule and any other provisions of this Contract relevant to security;

(b) identify the necessary delegated organisational roles defined for those responsible for ensuring it is complied with by the Supplier;

(c) detail the process for managing any security risks from Sub-Contractors and third parties authorised by the Customer with access to the Services, processes associated with the provision of the Services, the Customer Premises, the Sites and any ICT, Information and data (including the Customer’s Confidential Information and the Customer Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Services;

(d) unless otherwise specified by the Customer in writing, be developed to protect all aspects of the Services and all processes associated with the provision of the Services, including the Customer Premises, the Sites, and any ICT, Information and data (including the

Customer's Confidential Information and the Customer Data) to the extent used by the Customer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Services;

(e) set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Services and all processes associated with the provision 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 the provisions of this Contract;

(f) set out the plans for transitioning all security arrangements and responsibilities for the Supplier to meet the full obligations of the security requirements set out in this Contract and the Security Policy; and

(g) be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Customer engaged in the provision of the Services and shall only reference documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.

3.6 Amendment and Revision of the Security Management Plan

3.6.1 The Security Management Plan shall be fully reviewed and updated by the Supplier on the occasions listed below to ensure the Security Management Plan complies with the requirements of paragraph 3.5 and otherwise reflects any changes to the Supplier System, the Services or emerging information security best practices:

(a) each anniversary of the Commencement Date for the Contract Period;

(b) immediately following any material change to the Supplier System or Services and/or associated processes delivering the Solution;

(c) immediately following any change or proposed change to the Services and/or associated processes;

(d) immediately following any new perceived or changed security threats;

(e) upon the reasonable request of the Customer;

(f) immediately following a major incident; and

(g) immediately following any changes to the Security Policy.

3.6.2 The Supplier shall provide the Customer with the results of such reviews as soon as reasonably practicable after their completion and amendment of the Security Management Plan at no additional cost to the Customer. The results of the review shall include, without limitation:

(a) suggested improvements to the effectiveness of the Security Management Plan;

(b) updates to the risk assessments; and

(c) suggested improvements in measuring the effectiveness of controls.

3.6.3 Subject to paragraph 3.6.4, any change or amendment which the Supplier proposes to make to the Security Management Plan (as a result of a review carried out in accordance with paragraph 3.6.1, a request by the Customer or otherwise) shall be subject to the Variation Procedure and shall not be implemented until Approved by the Customer.

3.6.4 The Customer may, where it is reasonable to do so, Approve and require changes or amendments to the Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment for the purposes of this Contract.

4. BREACH OF SECURITY

4.1 Either party shall notify the other in accordance with the agreed security incident management process (as detailed in the Security Management Plan) upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.

4.2 Without prejudice to the security incident management process (as detailed in the Security Management Plan), upon becoming aware of any of the circumstances referred to in paragraph 4.1, the Supplier shall:

4.2.1 immediately take all reasonable steps(which shall include any action or changes reasonably required by the Customer) necessary to:

(a) minimise the extent of actual or potential harm caused by any Breach of Security;

(b) remedy such Breach of Security to the extent possible and protect the integrity of the Customer and the provision of the Services to the extent within its control against any such Breach of Security or attempted Breach of Security;

(c) prevent an equivalent breach in the future exploiting the same cause failure; and

(d) as soon as reasonably practicable provide to the Customer, where the Customer so requests, full details (using the reporting mechanism defined by the Security Management Plan if one exists) of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Customer.

4.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the Security Management Plan with the Security Policy or the requirements of this Schedule, then any required change to the Security Management Plan shall be at no cost to the Customer.

5. SECURITY TESTING

5.1 The Customer shall conduct Security Tests (including penetration tests) on the Solution from time to time. The Customer shall notify the Supplier of any under-performance

and of any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management) revealed by such Security Tests.

5.2 The Supplier shall promptly notify the Customer of any changes to the Solution and to the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such under-performance, failure or weakness. Subject to the Customer's prior written Approval, the Supplier shall implement such changes to the Solution and the Security Management Plan within the timetable set by the Customer or, if agreed with the Customer, provide the Customer with the fixes of such Security Tests (in a form approved by the Customer in advance) as soon as practicable after such notification.

5.3 The Customer shall repeat the relevant Security Tests. Without prejudice to any other right under the Contract, If any repeat Security Test carried out pursuant to this paragraph reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall constitute a material Default of this Contract

5.4 For the avoidance of doubt, where the change to the Solution or Security Management Plan is to address a non-compliance with the Security Policy or the requirements of this Schedule, the change to the Solution or Security Management Plan shall be at no cost to the Customer.

5.5 Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier’s ability to deliver the Services so as to meet the Service Level Performance Measures, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests.

ANNEX 1: SECURITY POLICY

[CUSTOMER WILL INSERT ITS SECURITY POLICY HERE]

ANNEX 2: SECURITY MANAGEMENT PLAN

[ ]