Department for Work & Pensions

THE SECRETARY OF STATE FOR WORK AND PENSIONS

TEST AND LEARN DPS

[Project_20559]

Version: 1.0

SCHEDULE C2

SECURITY REQUIREMENTS AND PLAN

1. Introduction

1.1 This Schedule covers;

a) Principles of security for the Supplier 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.

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

2.2 The Supplier shall be responsible for the security of the Supplier 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 Supplier System;

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 Supplier 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 Government Data;

b) loss of confidentiality of Government Data;

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

d) unauthorised access to network elements and buildings;

e) use of the Supplier System or Services by any third party in order to gain unauthorised access to any computer resource or Government Data;

f) loss of availability of Government Data due to any failure or compromise of the Services; and

g) loss of confidentiality, integrity and availability of Government Data through Cyber/internet threats.

3 Security Plan

Introduction

3.1 The Supplier shall develop, upload, implement and maintain a Security Plan to apply during the Contract Period which will be approved by the Buyer, tested, periodically updated and audited in accordance with this Schedule.

3.2 Where specified in the Order Form, the Supplier shall submit further detail regarding the information security measures they propose to use in delivery of this Contract. The Buyer will assess the data risk for this Contract and if the risk is deemed 'low' then the original questions answered as part of selection onto the DPS will be proportionate. If the data risk is assessed as higher, then the Supplier will be required to submit a security plan detailing, more specifically, the information security measures they propose to use in delivery of a specific contract.

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 Supplier will prepare and deliver to the Buyer for approval the full and final Security Plan as requested in the Order Form

3.4 If the Security Plan is approved by the Buyer it will be adopted immediately. If the Security Plan is not approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit to the Buyer 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 Buyer. If the Buyer does not approve the Security Plan following its resubmission, the matter will be resolved in accordance with Clause 45 (Resolving Disputes). No approval to be given by the Buyer 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 Supplier 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) those parts of the Specification relating to security;

d) ISO/IEC27002 and ISO/IEC27001 unless the Order Form states that these standards do not apply to this Contract; and

e) the data protection compliance guidance produced by the Buyer.

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 Supplier should notify the Buyer of such inconsistency immediately upon becoming aware of the same, and the Buyer shall, as soon as practicable, advise the Supplier which provision the Supplier 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 Buyer, a copy of the document will be made available to the Buyer upon request. The Security Plan shall be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the Services and shall not reference any other documents which are not either in the possession of the Buyer or otherwise specified in this Schedule.

Amendment and Revision

3.10 The Security Plan will be fully reviewed and updated by the Supplier from time to time to reflect:

a) emerging changes in Good Industry Practice;

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

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

d) a reasonable request by the Buyer.

3.11 The Supplier will provide the Buyer 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 Buyer.

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

4 Audit and Testing

4.1 The Supplier shall conduct tests of the processes and countermeasures contained in the Security Plan (**"Security Tests"**) as agreed by the Parties. The date, timing, content and conduct of such Security Tests shall be agreed in advance with the Buyer.

4.2 The Buyer shall be entitled to send a representative to witness the conduct of the Security Tests. The Supplier shall provide the Buyer with the results of such tests (in a form approved by the Buyer 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 Buyer pursuant to this Contract, the Buyer shall be entitled at any time and without giving notice to the Supplier to carry out such tests (including penetration tests) as it may deem necessary in relation to the Security Plan and the Supplier's compliance with and implementation of the Security Plan. The Buyer may notify the Supplier 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 Supplier 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 Supplier shall promptly notify the Buyer of any changes to the Security Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Buyer's approval in accordance with Paragraph 3.12, the Supplier shall implement such changes to the Security Plan in accordance with the timetable agreed with the Buyer 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 Buyer. For the purposes of this Paragraph 4, a weakness means a 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 This Paragraph 5 shall apply to this Contract unless the Order Form specifically states that the Supplier is not obliged to comply with ISO/IEC 27001.

5.2 The Supplier 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 Buyer any associated security audit reports and shall otherwise notify the Buyer of the results of such security audits.

5.3 If it is the Buyer's reasonable opinion that compliance with the principles and practices of ISO 27001 is not being achieved by the Supplier, then the Buyer shall notify the Supplier of the same and give the Supplier 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 Supplier does not become compliant within the required time then the Buyer 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 5.3 the Supplier is found to be non-compliant with the principles and practices of ISO 27001 then the Supplier 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 Buyer 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 Supplier shall:

a) immediately take all reasonable steps necessary to;

(i) remedy such breach or protect the Supplier 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 Buyer. In the event that such action is taken in response to a breach that is determined by the Buyer acting reasonably not to be covered by the obligations of the Supplier under this Contract, then the Supplier shall be entitled to refer the matter to the change control procedure in Clause 35 (Changing the Contract); and

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