

Call-Off Schedule 9 (Security)

Part A: Short Form Security Requirements

1. Definitions

- 1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Breach of Security"	the occurrence of: a) any unauthorised access to or use of the Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Authority and/or the Supplier in connection with this Contract; and/or b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Authority and/or the Supplier in connection with this Contract, in either case as more particularly set out in the Security Policy where the Authority has required compliance therewith in accordance with Paragraph 2.1;
"Security Management Plan"	the Supplier's security management plan prepared pursuant to this Schedule, a draft of which has been provided by the Supplier to the Authority and has been updated from time to time.

2. Complying With Security Requirements And Updates To Them

- 2.1 The Supplier shall comply with the requirements in this Schedule in respect of the Security Management Plan. Where specified by the Authority when it has undertaken a Further Competition it shall also comply with the Security Policy and ICT Policy and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy.
- 2.2 Where the Security Policy applies the Authority shall notify the Supplier of any changes or proposed changes to the Security Policy.
- 2.3 If the Supplier believes that a change or proposed change to the Security Policy will have a material and unavoidable cost implication to the provision of the Deliverables, it may propose a Variation to the Authority. In doing so, the Supplier must support its request by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs. Any change to the Charges shall be subject to the Variation Procedure.
- 2.4 Until and/or unless a change to the Charges is agreed by the Authority pursuant to the Variation Procedure the Supplier shall continue to provide the Deliverables in accordance with its existing obligations.

3. Security Standards

- 3.1 The Supplier acknowledges that the Authority places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on security.
- 3.2 The Supplier shall be responsible for the effective performance of its security obligations

and shall at all times provide a level of security which:

- 3.2.1 is in accordance with the Law and this Contract;
- 3.2.2 as a minimum demonstrates Good Industry Practice;
- 3.2.3 meets any specific security threats of immediate relevance to the Deliverables and/or the Government Data; and
- 3.2.4 where specified by the Authority in accordance with Paragraph 2.1 complies with the Security Policy and the ICT Policy.
- 3.2.5 complies with the 14 Cloud Security Principles available at: <https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles>. The Supplier must document how it and any cloud service providers they use comply with these principles, and provide this documentation upon request by the Authority.

3.3 The references to standards, guidance and policies contained or set out in Paragraph The Supplier shall be responsible for the effective performance of its security obligations and shall at all times provide a level of security which: 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.

3.4 In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Supplier 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 Supplier which provision the Supplier shall be required to comply with.

4. **Security Management Plan**

4.1 **Introduction**

4.1.1 The Supplier shall develop and maintain a Security Management Plan in accordance with this Schedule. The Supplier shall thereafter comply with its obligations set out in the Security Management Plan.

4.2 **Content of the Security Management Plan**

4.2.1 The Security Management Plan shall:

- a) comply with the principles of security set out in Paragraph **Security Standards** and any other provisions of this Contract relevant to security;
- b) identify the necessary delegated organisational roles for those responsible for ensuring it is complied with by the Supplier;
- c) detail the process for managing any security risks from Subcontractors and third parties authorised by the Authority with access to the Deliverables, processes associated with the provision of the Deliverables, the Authority Premises, the Sites and any ICT, Information and data (including the Authority's Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;
- d) be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Authority Premises, the Sites, and any ICT, Information and data (including the Authority's Confidential Information and the Government Data) to the extent used by the Authority 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 Deliverables;
- e) set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the provision of the Goods and/or Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables 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, where necessary in accordance with Paragraph The Supplier shall comply with the requirements in this Schedule in respect of the Security Management Plan. Where specified by the Authority when it has undertaken a Further Competition it shall also comply with the Security Policy and ICT Policy and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy. the Security Policy; and
- g) be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Authority engaged in the provision of the Deliverables and shall only reference documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.

4.3 Development of the Security Management Plan

- 4.3.1 Within 20 Working Days after the Start Date and in accordance with Paragraph **Amendment of the Security Management Plan**, the Supplier shall prepare and deliver to the Authority for Approval a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan.
- 4.3.2 If the Security Management Plan submitted to the Authority in accordance with Paragraph Within 20 Working Days after the Start Date and in accordance with Paragraph **Amendment of the Security Management Plan**, the Supplier shall prepare and deliver to the Authority for Approval a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan., or any subsequent revision to it in accordance with Paragraph **Amendment of the Security Management Plan**, is Approved it will be adopted immediately and will replace the previous version of the Security Management Plan and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not Approved, the Supplier shall amend it within 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 15 Working Days from the date of its first submission to the Authority. If the Authority does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure.
- 4.3.3 The Authority shall not unreasonably withhold or delay its decision to Approve or not the Security Management Plan pursuant to Paragraph If the Security Management Plan submitted to the Authority in accordance with Paragraph Within 20 Working Days after the Start Date and in accordance with Paragraph **Amendment of the Security Management Plan**, the Supplier shall prepare and deliver to the Authority for Approval a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan., or any subsequent revision to it in accordance with Paragraph **Amendment of the Security Management Plan**, is Approved it will be adopted immediately and will replace the previous version of the Security Management Plan and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not Approved, the Supplier shall amend it within 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 15 Working Days from the date of its first submission to the Authority. If the Authority does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure.. However, a refusal by the Authority to Approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph **Content of the Security Management Plan**

shall be deemed to be reasonable.

- 4.3.4 Approval by the Authority of the Security Management Plan pursuant to Paragraph If the Security Management Plan submitted to the Authority in accordance with Paragraph Within 20 Working Days after the Start Date and in accordance with Paragraph **Amendment of the Security Management Plan**, the Supplier shall prepare and deliver to the Authority for Approval a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan., or any subsequent revision to it in accordance with Paragraph **Amendment of the Security Management Plan**, is Approved it will be adopted immediately and will replace the previous version of the Security Management Plan and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not Approved, the Supplier shall amend it within 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 15 Working Days from the date of its first submission to the Authority. If the Authority does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure. or of any change to the Security Management Plan in accordance with Paragraph **Amendment of the Security Management Plan** shall not relieve the Supplier of its obligations under this Schedule.

4.4 **Amendment of the Security Management Plan**

- 4.4.1 The Security Management Plan shall be fully reviewed and updated by the Supplier at least annually to reflect:
- a) emerging changes in Good Industry Practice;
 - b) any change or proposed change to the Deliverables and/or associated processes;
 - c) where necessary in accordance with Paragraph The Supplier shall comply with the requirements in this Schedule in respect of the Security Management Plan. Where specified by the Authority when it has undertaken a Further Competition it shall also comply with the Security Policy and ICT Policy and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy., any change to the Security Policy;
 - d) any new perceived or changed security threats; and
 - e) any reasonable change in requirements requested by the Authority.
- 4.4.2 The Supplier shall provide the Authority 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 Authority. 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.
- 4.4.3 Subject to Paragraph The Authority may, acting reasonably, 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., 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 The Security Management Plan shall be fully reviewed and updated by the Supplier at least annually to reflect:, a request by the Authority or otherwise) shall be subject to the Variation Procedure.

- 4.4.4 The Authority may, acting reasonably, 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.

5. Security Breach

- 5.1 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.
- 5.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 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., the Supplier shall:
- 5.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Authority) 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 Authority and the provision of the Goods and/or 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 Authority, where the Authority so requests, full details (using the reporting mechanism defined by the Security Management Plan) of the Breach of Security or attempted Breach of Security, including a cause analysis where required by the Authority.
- 5.3 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 (where relevant in accordance with Paragraph The Supplier shall comply with the requirements in this Schedule in respect of the Security Management Plan. Where specified by the Authority when it has undertaken a Further Competition it shall also comply with the Security Policy and ICT Policy and shall ensure that the Security Management Plan produced by the Supplier fully complies 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 Authority.