**Call-Off Schedule 9 (Security)**

**Part A: Short Form Security Requirements**

1. **Definitions**
	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:* 1. 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 UKEF and/or the Supplier in connection with this Contract; and/or
	2. 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 UKEF and/or the Supplier in connection with this Contract,

in either case as more particularly set out in the Security Policy where UKEF has required compliance therewith in accordance with paragraph 2.2; |
| **"Security Management Plan"**  | the Supplier's security management plan prepared pursuant to this Schedule (if required), as updated from time to time. |

1. **Complying with security requirements and updates to them**

* 1. The Supplier shall comply with the requirements in this Schedule in respect of the Security Management Plan and the additional baseline security requirements set out in Annex 1 of this Schedule. Where specified by UKEF in an Order Form, the Supplier shall also comply with the Security Policy (if any) and shall produce a Security Management Plan which fully complies with the Security Policy.
	2. Where the Security Policy applies UKEF shall notify the Supplier of any changes or proposed changes to the Security Policy.
	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 UKEF. 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.
	4. Until and/or unless a change to the Charges is agreed by UKEF pursuant to the Variation Procedure the Supplier shall continue to provide the Deliverables in accordance with its existing obligations.

1. **Security Standards**
	1. The Supplier acknowledges that UKEF places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on security.

* 1. The Supplier shall be responsible for the effective performance of its security obligations and shall at all times provide a level of security which:
		1. is in accordance with the Law and this Contract;
		2. as a minimum demonstrates Good Industry Practice;
		3. meets any specific security threats of immediate relevance to the Deliverables and/or the Government Data; and
		4. where specified by UKEF in accordance with paragraph 2.2complies with the Security Policy and the ICT Policy.
	2. The references to standards, guidance and policies contained or set out in Paragraph 3.2 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. In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Supplier should notify UKEF's Representative of such inconsistency immediately upon becoming aware of the same, and UKEF's Representative shall, as soon as practicable, advise the Supplier which provision the Supplier shall be required to comply with.
1. **Security Management Plan**

* 1. **Introduction**

* + 1. If required by UKEF in the Order Form, 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 in respect of the relevant Call-Off Contract.

* 1. **Content of the Security Management Plan**

* + 1. If required by UKEF in the Order Form, the Security Management Plan shall:
			1. comply with the principles of security set out in Paragraph 3 andany other provisions of this Contract relevant to security;
			2. identify the necessary delegated organisational roles for those responsible for ensuring it is complied with by the Supplier;
			3. detail the process for managing any security risks from Subcontractors (which includes Affiliate Firms) and third parties authorised by UKEF with access to the Deliverables, processes associated with the provision of the Deliverables, UKEF Premises, the Sites and any ICT, Information and data (including UKEF’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;
			4. be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including UKEF Premises, the Sites, and any ICT, Information and data (including UKEF’s Confidential Information and the Government Data) to the extent used by UKEF 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;
			5. 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 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;

* + - 1. 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 2.2the Security Policy; and

* + - 1. be written in plain English in language which is readily comprehensible to the staff of the Supplier and UKEF 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.

* 1. **Development of the Security Management Plan**

* + 1. If required by UKEF in the Order Form, within twenty (20)Working Days after the Start Date and in accordance with Paragraph 4.4, the Supplier shall prepare and deliver to UKEF for Approval a fully complete and up to date Security Management Plan in respect of the relevant Call-Off Contract.

* + 1. If the Security Management Plan submitted to UKEF in accordance with Paragraph 4.3.1or any subsequent revision to it in accordance with Paragraph 4.4, 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 ten (10) Working Days of a notice of non-approval from UKEF and re-submit to UKEF 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 from the date of its first submission to UKEF. If UKEF does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure.

* + 1. UKEF shall not unreasonably withhold or delay its decision to Approve or not the Security Management Plan pursuant to Paragraph 4.3.2. However a refusal by UKEF to Approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2shall be deemed to be reasonable.
		2. Approval by UKEF of the Security Management Plan pursuant to Paragraph 4.3.2or of any change to the Security Management Plan in accordance with Paragraph 4.4shall not relieve the Supplier of its obligations under this Schedule.

* 1. **Amendment of the Security Management Plan**

* + 1. The Security Management Plan (if required by UKEF in respect of a Call-Off Contract) shall be fully reviewed and updated by the Supplier at least annually to reflect:
			1. emerging changes in Good Industry Practice;
			2. any change or proposed change to the Deliverables and/or associated processes;
			3. where necessary in accordance with paragraph 2.2, any change to the Security Policy;
			4. any new perceived or changed security threats; and
			5. any reasonable change in requirements requested by UKEF.

* + 1. The Supplier shall provide UKEF 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 UKEF. The results of the review shall include, without limitation:
			1. suggested improvements to the effectiveness of the Security Management Plan;
			2. updates to the risk assessments; and
			3. suggested improvements in measuring the effectiveness of controls.

* + 1. Subject to Paragraph 4.4.4, 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 4.4.1, a request by UKEF or otherwise) shall be subject to the Variation Procedure.

* + 1. UKEF 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.
1. **Security breach**

* 1. Either Party shall notify the other upon becoming aware of any Breach of Security or any potential or attempted Breach of Security. Such notification shall be in accordance with the agreed security incident management process (as detailed in the Security Management Plan), if applicable.

* 1. Without prejudice to any security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 5.1, the Supplier shall:

* + 1. immediately take all reasonable steps (which shall include any action or changes reasonably required by UKEF) necessary to:
			1. minimise the extent of actual or potential harm caused by any Breach of Security;
			2. remedy such Breach of Security to the extent possible and protect the integrity of UKEF and the provision of the Services to the extent within its control against any such Breach of Security or attempted Breach of Security;
			3. prevent an equivalent breach in the future exploiting the same cause failure; and
			4. as soon as reasonably practicable provide to UKEF, where UKEF 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 UKEF.
	1. 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 2.2) or the requirements of this Schedule, then any required change to the Security Management Plan shall be at no cost to UKEF.

**Annex 1 – Additional UKEF Baseline security requirements**

UKEF takes the security of all its assets very seriously including Information, Personnel, and physical assets and the information outlined in this schedule contributes to ensuring all risks, breaches or incidents are managed appropriately.

All UKEF third party suppliers must maintain an appropriate level of security to ensure the protection of UKEF assets throughout the duration of the contract and to safeguard UKEF assets from any unauthorised access, loss or disclosure of information handled in respect of the contact.

**Security Policy**

UKEF has security policies and procedures for the protection of all assets including detecting, reporting, responding to and handling security incidents and breaches. If so required, Suppliers must adhere to UKEF protective security requirements to ensure they manage risks and protect UKEF assets when handling them on behalf of UKEF - (This will include any sub-contractors).

**Information Security**

Information security is the preservation of confidentiality, integrity and availability of UKEF information. It may also include the authenticity, accountability, non-repudiation and reliability of information.

**Government Security Classifications Policy**

Suppliers handling UKEF information must do so in accordance with the HMG Security Classifications Policy and designated handling instructions:

**OFFICIAL**

The supplier must ensure all personnel having access to UKEF OFFICIAL information have undergone basic recruitment checks (further details given below in Personnel Security).

Access to OFFICIAL information with the OFFICIAL-SENSITIVE handling caveat must be confined to individuals on a “need-to-know” basis and whose access is essential for the purpose of their duties.

**UK SENSITIVE INFORMATION**

Information will only be handled by a Supplier where UKEF has notified the Supplier prior to receipt of this information and the supplier must implement measures as agreed with UKEF in order to ensure that information is safeguarded in accordance with the applicable Government Standards and UKEF policy & procedures.

**Risk Management and Security Management Plan**

A Security Management Plan will be required from the Supplier where work is identified as being high risk. This should be developed and maintained for the duration of the contract period.

**Legislative, Regulatory and Contractual Requirements**

UKEF requires the security of its information to be maintained in order to ensure reliability of its information for business needs; to meet statutory; regulatory; legislative and policy obligations. Suppliers handling UKEF information must do so in accordance with relevant legislation.

If the Supplier shares UKEF information, it will be subject to a confidentiality clause or non-disclosure agreement and subject to the Official Secrets Act.

* Where relevant the following legislation may apply:
* Data Protection Act 2018 (GDPR)
* Public Records Acts 1958
* Freedom of Information Act 2000
* Environmental Information Regulations 2004
* Human Rights Act 1998
* Computer Misuse Act 1990
* Copyright (Computer Programs) Regulations
* Communications Act 2003
* Regulation of Investigatory Powers Act 2000

The Codes of conduct for suppliers outline the standards and behaviours that the government expects of all suppliers and grant recipients.

**General Data Protection Regulation (GDPR)**

If the Supplier handles personal data a ‘Data Privacy Impact Assessment’ (DPIA) will be carried out. The DPIA assesses the risks against the GDPR and UKEF legal requirements.

**Access to UKEF Information & Systems**

If the Supplier is granted access to UKEF information assets and systems, it must comply with the requirements of the UKEF Acceptable Use Policy. Failure to comply with these policies and other relevant instructions may constitute a breach of contract and lead to termination or legal action.

**Information Assurance Questionnaire**

If the Supplier is required to handle UKEF data on behalf of UKEF then a cyber security risk assessment will be carried out if so required by UKEF.

The Cyber and Information Assurance Questionnaire is a series of questions which seeks to identify the risks and establish what security controls are required.

**Physical Security**

Where the service delivery is to be carried out on the Supplier’s own premises or buildings, the Supplier must have policies and building facilities, which protect UKEF assets and maintain the principle standards for protection at the OFFICIAL level for relevant working space. Including appropriate security policies in adherence to UKEF security practices e.g.

* Clear desk & Screen policy for all staff with access to UKEF information must be followed;
* Suitable secure storage facilities must be provided;
* Policy for working with and the secure movement (internally), or transportation (externally) of sensitive material must be followed;
* Only staff with the need to know should have access to UKEF information;
* Disposal and destruction facilities must be appropriate for the classification level of the information.

**Data Loss and Incident Management & Response**

The Supplier must have a security incident reporting process in place to ensure that any incidents involving UKEF information or business are immediately reported to UKEF. The Supplier must undertake any remedial action required by UKEF and ensure that this is implemented in an auditable way. Any security incident involving OFFICIAL-SENSITIVE information or above and/or personal information, must be immediately reported to UKEF.