# TRADER SUPPORT SERVICE

## SCHEDULE 2.4

## SECURITY MANAGEMENT

**Security Management**

**1 DEFINITIONS**

In this Schedule, the following definitions shall apply:

| | |
|---|---|
| **"Breach of Security"** | the occurrence of:<br><br>(a) any unauthorised access to or use of the Services, the Authority Premises, the Sites, the Supplier System, the Authority System (to the extent that it is under the control of the Supplier) and/or any IT, information or data (including the Confidential Information and the Authority Data) used by the Authority and/or the Supplier in connection with this Agreement; and/or<br><br>(b) the loss, corruption and/or unauthorised disclosure of any information or data (including the Confidential Information and the Authority Data), including any copies of such information or data, used by the Authority and/or the Supplier in connection with this Agreement; and/or<br><br>(c) a failure to comply with the personnel security requirements, as set out in the Security Management Plan,<br><br>in each case as may be more particularly set out in the security requirements in Schedule 2.1 (Services Description) and the Baseline Security Requirements; |
| **"CESG"** | the UK Government's national technical authority for information assurance; |
| "**CPA**" | the CESG Commercial Product Assurance scheme; |
| "**Off-Shore Personnel**" | (i) the Supplier Personnel in the Supplier's Global Delivery Centre in Poland; |

| | | |
|---|---|---|
| | (ii) | any Supplier Personnel of a Sub-contractor working off-shore; and |
| | (iii) | other off-shore Supplier Personnel as identified pursuant to a Change; |
| "**Off-Shore Personnel Security Checks**" | (a) | for limb (i) of the definition of Off-Shore Personnel, the security checks set out in Annex 3; and |
| | (b) | any security checks identified and agreed as required pursuant to limbs (ii) and (iii) of the definition of Off-Shore Personnel; |
| **"Security Policy Framework"** | the Security Policy Framework published by the Cabinet Office as updated from time to time including any details notified by the Authority to the Supplier; | |

## 2 SECURITY REQUIREMENTS

2.1 The Supplier shall comply with the Baseline Security Requirements and the Security Management Plan and the Supplier shall ensure that its Security Management Plan fully complies with the Baseline Security Requirements and the Security Policy Framework.

2.2 The Authority shall notify the Supplier of any changes or proposed changes to the Baseline Security Requirements.

2.3 If the Supplier believes that a change or proposed change to the Baseline Security Requirements will have a material and unavoidable cost implication to the Services it may submit a Change Request. 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 then be agreed in accordance with the Change Control Procedure.

2.4 Until and/or unless a change to the Charges is agreed by the Authority pursuant to the Change Control Procedure the Supplier shall continue to perform the Services in accordance with its existing obligations.

## 3 PRINCIPLES OF SECURITY

3.1 The Supplier acknowledges that the Authority places great emphasis on the reliability of the performance of the Services, 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:

(a) is in accordance with the Law and this Agreement;

(b) demonstrates Good Industry Practice;

(c) meets specific security threats of immediate relevance to the Services and/or the Authority Data; and

(d) complies with the Baseline Security Requirements and the Authority's specific security requirements as described in the Services Description as appropriate.

3.3 In the event of any inconsistency in the provisions of the standards, guidance and requirements listed in Paragraph 3.2 above, 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 MALICIOUS SOFTWARE

4.1 The Supplier shall, as an enduring obligation throughout the Term and at no cost to the Authority, use the latest versions of anti-virus definitions and software available from an industry accepted anti-virus software vendor (unless otherwise agreed in writing between the Parties) to check for, contain the spread of, and minimise the impact of Malicious Software in the IT Environment (or as otherwise agreed by the Parties). The Supplier may be required to provide details of the version of anti-virus software being used in certain circumstances, e.g. in response to a specific threat.

4.2 Notwithstanding Paragraph 4.1, if Malicious Software is found, the Parties shall co-operate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Authority Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.

4.3 Any cost arising out of the actions of the Parties taken in compliance with the provisions of Paragraph 4.2 shall be borne by the Parties as follows:

(a) by the Supplier where the Malicious Software originates from the Software (except where the Authority has waived the obligation set out in Paragraph 4.1) or the Authority Data (whilst the Authority Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Authority when provided to the Supplier; and

(b) otherwise by the Authority.

## 5 SECURITY MANAGEMENT PLAN

5.1 Within twenty (20) Working Days after the signature of the Agreement, the Supplier shall prepare and submit to the Authority for approval in accordance with Paragraph 5.3 a fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of Paragraph 5.2.

5.2 The Security Management Plan shall:

(a) be based on the Supplier's final response to the Authority's Security Questionnaire, a copy of which is set out in Annex 2;

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

(c) detail the process for vetting staff at the appropriate security level with reference to the level of access staff will have to Authority Data, managing any security risks from Sub-contractors and third parties authorised by the Authority with access to the Services, processes associated with the delivery of the Services, the Authority Premises, the Sites, the Supplier System, the Authority System (to extent that it is under the control of the Supplier) and any IT, Information and data (including the Authority Confidential Information and the Authority 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 Authority in writing, be developed to protect all aspects of the Services and all processes associated with the delivery of the Services, including the Authority Premises, the Sites, the Supplier System, the Authority System (to the extent that it is under the control of the Supplier) and any IT, Information and data (including the Authority Confidential Information and the Authority Data) to the extent used by the Authority or the Supplier in connection with this Agreement 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 delivery of the Services and 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 Schedule;

(f) set out the plans for transiting all security arrangements and responsibilities for the Supplier to meet the full obligations of the security requirements set out in Schedule 2.1 (*Services Description*) and this Schedule;

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

5.3 If the Security Management Plan submitted to the Authority Representative pursuant to Paragraph 5.1 is approved by the Authority Representative, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not approved by the Authority Representative, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Authority and re-submit it to the Authority Representative for approval. The Parties shall 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 Representative. If the Authority Representative does not approve the Security Management Plan following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Authority Representative pursuant to this Paragraph 5.3 may be unreasonably withheld or delayed. However any failure to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 5.2 shall be deemed to be reasonable.

5.4 Approval by the Authority of the Security Management Plan pursuant to Paragraph 5.3 or of any change or amendment to the Security Management Plan shall not relieve the Supplier of its obligations under this Schedule.

## 6 AMENDMENT AND REVISION OF THE SECURITY MANAGEMENT PLAN

6.1 The Security Management Plan shall be fully reviewed and updated by the Supplier within ten (10) Working Days of any Breach of Security and further at least annually to reflect:

(a) emerging changes in Good Industry Practice;

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

(c) any new perceived or changed security threats; and

(d) any reasonable change in requirements requested by the Authority.

6.2 The Supplier shall provide the Authority with the results of such reviews as soon as reasonably practicable after their completion and amend 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;

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

6.3 Subject to Paragraph 6.4, any change which the Supplier proposes to make to the Security Management Plan (as a result of a review carried out pursuant to Paragraph 6.1, an Authority request, a change to Schedule 2.1 (*Services Description*) or otherwise) shall be subject to the Change Control Procedure.

6.4 The Authority 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 Change Control Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Change Control Procedure for the purposes of formalising and documenting the relevant change or amendment.

## 7 BREACH OF SECURITY

7.1 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 attempted Breach of Security.

7.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 7.1, the Supplier shall:

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

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

(ii) remedy such Breach of Security to the extent possible and protect the integrity of the IT Environment to the extent within its control against any such Breach of Security or attempted Breach of Security;

(iii) prevent a further Breach of Security or attempted Breach of Security in the future exploiting the same root cause failure; and

(iv) supply any data regarding, affected by or related to the Breach of Security or attempted breach of Security which it is reasonable to be requested to the Authority or the Computer Emergency Response Team for UK Government ("GovCertUK") on the Authority's request within two (2) Working Days and without charge (where such requests are reasonably related to a possible incident or compromise);

(b) as soon as reasonably practicable provide to the Authority full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Authority; and

(c) maintain auditable records of such Breach of Security in accordance with Schedule 8.4 (Reports and Records).

7.3 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 Baseline Security Requirements or security requirements (as set out in Schedule 2.1 (*Services Description*)) or the requirements of this Schedule, then any required change to the Security Management Plan shall be at no cost to the Authority.

## ANNEX 1: BASELINE SECURITY REQUIREMENTS

### 1 Higher Classifications

1.1 The Supplier shall not handle Authority information classified SECRET or TOP SECRET except if there is a specific requirement and in this case prior to enabling the Supplier to have access to such SECRET or TOP SECRET information, the Authority shall provide the Supplier with specific guidance regarding how the information is to be handled.

### 2 End User Devices

2.1 When Authority Data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or system component which has been formally assured through a recognised certification process of the CESG to at least Foundation Grade, for example, under CPA.

2.2 Devices used to access or manage Authority Data and services must be under the management authority of Authority or Supplier and have a minimum set of security policy configuration enforced. These devices must be placed into a 'known good' state prior to being provisioned into the management authority of the Authority. Unless otherwise agreed with the Authority in writing, all Supplier devices are expected to meet the set of security requirements set out in the CESG End User Devices Platform Security Guidance (https://www.ncsc.gov.uk/collection/end-user-device-securityAs a minimum, the security standards must include Assurance Framework, Ten Critical Steps and Requirements. Where the guidance highlights shortcomings in a particular platform the Supplier may wish to use, then these should be discussed with the Authority and a joint decision shall be taken on whether the residual risks are acceptable. Where the Supplier wishes to deviate from the CESG guidance, then this should be agreed in writing on a case by case basis with the Authority.

### 3 Data Processing, Storage, Management and Destruction

3.1 The Supplier and Authority recognise the need for the Authority's information to be safeguarded under the UK Data Protection regime or a similar regime. To that end, the Supplier must be able to state to the Authority the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks Authority information will be subject to at all times.

3.2 The Supplier shall agree any change in location of data storage, processing and administration with the Authority in advance where the proposed location is outside the UK. The Authority's agreement to any such change shall be entirely at the Authority's discretion and, in so far as the change in location entails the transfer of Personal Data to a location outside the UK, shall only be given if a Change Request is expressly permitted by Paragraph 1.8 of Schedule 2.8 (*Data Processing and List of Sub-processors*).

3.3 The Supplier shall:

(a) provide the Authority with all Authority Data on demand in an agreed open format;

(b) have documented processes to guarantee availability of Authority Data in the event of the Supplier ceasing to trade;

(c) securely destroy all media that has held Authority Data at the end of life of that media in line with Good Industry Practice; and

(d) securely erase any or all Authority Data held by the Supplier when requested to do so by the Authority.

**4 Networking**

4.1 The Authority requires that any Authority Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted using a product or system component which has been formally assured through a certification process recognised by CESG, to at least Foundation Grade, for example, under CPA or through the use of pan-government accredited encrypted networking services via the Public Sector Network ("PSN") framework (which makes use of Foundation Grade certified products).

4.2 The Authority requires that the configuration and use of networking equipment to provide the Services, including those that are located in secure physical locations, are at least compliant with Good Industry Practice.

**5 Security Architectures**

5.1 The Supplier shall apply the 'principle of least privilege' (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of IT systems which will process or store Authority Information.

5.2 When designing and configuring the IT Environment (to the extent that the IT Environment is within the control of the Supplier) the Supplier shall follow Good Industry Practice, including seeking guidance from recognised security professionals with the appropriate skills, for all bespoke or complex components of the Supplier Solution.

**6 Personnel Security**

6.1 Supplier Personnel shall be subject to pre-employment checks that include, as a minimum: identity, unspent criminal convictions and right to work (including nationality and immigration status).

6.2 The Supplier shall agree on a case by case basis Supplier Personnel roles which require specific government clearances (such as 'SC') including system administrators with privileged access to IT systems which store or process Authority Data.

6.3 The Supplier shall prevent Supplier Personnel who are unable to obtain the required security clearances from accessing systems which store, process, or are used to manage Authority Data except where agreed with the Authority in writing.

6.4 All Supplier Personnel that have the ability to access Authority Data or systems holding Authority Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Authority in writing, this training must be undertaken annually.

6.5 Where the Supplier or Sub-Contractors grants increased IT privileges or access rights to Supplier Personnel, those Supplier Personnel shall be granted only those permissions necessary for them to carry out their duties. When staff no longer need elevated privileges or leave the organisation, their access rights shall be revoked within 2 Working Days.

6.6 Notwithstanding the Supplier's obligation to assure that the Security Management Plan is implemented and followed, the Supplier shall require that the Supplier Personnel are promptly informed of action taken in relation to any failure to do so.

6.7 The Supplier shall manage that Supplier Personnel complete the security questionnaire as provided by the Authority from time to time.

6.8 The Supplier shall perform the Off-Shore Personnel Security Checks in relation to any proposed Off-Shore Personnel prior to their engagement to the reasonable satisfaction of the Authority in the delivery of the Services under this Agreement.

**7 Identity, Authentication and Access Control**

7.1 The Supplier shall operate an access control regime to ensure all users and administrators of the Supplier Solution are uniquely identified and authenticated when accessing or administering the Services. Applying the 'principle of least privilege', users and administrators shall be allowed access only to those parts of the Supplier Solution they require. The Supplier shall retain an audit record of accesses.

**8 Audit and Monitoring**

8.1 The Supplier shall collect audit records which relate to security events in the systems or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include:

(a) Logs to facilitate the identification of the specific asset which makes every outbound request external to the IT Environment (to the extent that the IT Environment is within the control of the Supplier). To the extent the design of the Supplier Solution and Services allows such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers.

(b) Security events generated in the IT Environment (to the extent that the IT Environment is within the control of the Supplier) and shall include: privileged account logon and logoff events, the start and termination of remote access sessions, security alerts from desktops and server operating systems and security alerts from third party security software.

8.2 The Supplier and the Authority shall work together to establish any additional audit and monitoring requirements for the IT Environment.

8.3 The Supplier shall retain audit records collected in compliance with Paragraph 8.1 for a period of at least six (6) months.

**ANNEX 2**

Annex 2 of Schedule 2.4 has been withdrawn for Freedom of Information Act purposes.

**ANNEX 3: OFF-SHORE PERSONNEL SECURITY CHECKS**

1. IDENTITY - Confirmation of Identity - mandatory

2. RIGHT to WORK - Confirmation of the individual's right to work in the Country of employment – mandatory

3. RESIDENCE - Confirmation of current address - mandatory

4. EMPLOYMENT HISTORY - Verification of the last 5 years of occupational history – Mandatory

(Note: Employees in Poland are not subject to Criminal Record or Finance checks as these are illegal for employment purposes. )