# PICTS Contract Schedule 7 Security

**Document Info**

**Version #:** 1.0

**Date:** 15 December 2016

**Revision History**

| Version | Date | Details of Changes | Author |
|---|---|---|---|
| 0.1 | 1/11/16 | First draft based on RM1058 schedule | Sopra Steria |
| 0.2 | 06/12/16 | Update following Security Review | Sopra Steria |
| 0.3 | 07/12/16 | Update and inclusion of new words from Security Review with Authority | Sopra Steria |
| 0.4 | 09/12/16 | Internal review from Sopra Steria Security Practise and account team | Sopra Steria |
| 0.5 | 13/12/16 | Correction of formatting problem plus update to accept changes following MoJ IA review | Sopra Steria |
| 0.6 | 15/12/16 | Joint review | Sopra Steria and MoJ |
| 1.0 | 15/12/16 | Final version for completion | Sharpe Pritchard |

## 1. DEFINITIONS

**1.1** In this Schedule 7, the following definitions shall apply:

| | |
|---|---|
| **"Accreditation Standards"** | means complying with HMG Information Assurance Standards 1-6 and Security Policy Framework Tiers 1-4, all of which are accessible on the NSCS website; |
| **"Baseline Security Requirements"** | means those requirements outlined in Annex 1 of this Schedule 7 |
| **"Breach of Security"** | means the occurrence of:<br>a) any unauthorised access to or use of the Services, the Locations, the System and/or any ICT, information or data (including the Confidential Information and the AUTHORITY Data) used by the AUTHORITY and/or the PROVIDER in connection with this Agreement; and/or<br>b) the loss 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 PROVIDER in connection with this Agreement,<br>in either case as more particularly set out in:<br>(1) the Baseline Security Requirements in Annex 1 to this Schedule 7. |
| **"Good Industry Practice"** | means following HMG security standards including Information Assurance Standards 1-6, Security Policy Framework Tiers 1-4 and vendor best practice where HMG standards do not define solutions; |
| **"ISMS"** | the information security management system developed by the PROVIDER in accordance with paragraph 2 (ISMS) as updated from time to time in accordance with this Schedule 7; |
| **"Security Management Plan"** | the PROVIDER's security management plan prepared pursuant to paragraph 6 of this Schedule 7, as updated from time to time; |
| **"Security Policy Framework"** | the HMG Security Policy Framework https://www.gov.uk/government/publications/security-policy-framework; and |
| **"Security Tests"** | has the meaning given in paragraph 8.1 of this Schedule (Testing of the ISMS). |

## 2. INTRODUCTION

**2.1** The Parties acknowledge that the purpose of the ISMS and the Security Management Plan are to ensure a good organisational approach to security under which the specific requirements of this Agreement will be met.

**2.2** The AUTHORITY shall clearly articulate its high level security requirements so that the PROVIDER can ensure that the ISMS, security related activities and any mitigations are driven by these fundamental needs.

**2.3** Both Parties shall provide a reasonable level of access to any members of their personnel for the purposes of designing, implementing and managing security.

**2.4** The PROVIDER shall use as a minimum, Good Industry Practice, in the day to day operation of any system holding, transferring or processing AUTHORITY Data and any system that could directly or indirectly have an impact on that information, and shall ensure that the AUTHORITY Data remains under the effective control of the PROVIDER at all times.

**2.5** The PROVIDER shall ensure the up-to-date maintenance of a security policy relating to the operation of its own organisation and system and on request shall supply this document as soon as practicable to the AUTHORITY.

**2.6** The AUTHORITY and the PROVIDER acknowledge that information security risks are shared between the Parties and that a compromise of either the PROVIDER or the AUTHORITY's security provisions represents an unacceptable risk to the AUTHORITY requiring immediate communication and co-operation between the Parties.

## 3. ACCREDITATION

**3.1** The PROVIDER will manage accreditation activities in relation to the Services that it provides which will include:

3.1.1 Provision of appropriately skilled individuals to support the creation of the Risk Management Accreditation Document Set (RMADS) for the services within the scope of the PROVIDER;

3.1.2 Management of all identified Risks to the successful operation of the Services, utilising the AUTHORITY's risk assessment tool, to the satisfaction of the AUTHORITY and specifically the Accreditor by means of Risk Management;

3.1.3 Management of the coordination of IT Health Checks (ITHC) to support accreditation including the creation of scoping documents as defined in Section 9; and

3.1.4 The provision of 30 man-days of IT Health Checks (ITHC) per annum with any deficiencies documented within the RMADS.

**3.2** The PROVIDER will provide accreditable solutions and services in line with the Accreditation Standards.

## 4. PUBLIC SERVICES NETWORK (PSN)

**4.1** The PROVIDER will support the AUTHORITY in completing and submitting its PSN Code of Connection (PSN CoCo).

**4.2** Where the PROVIDER delivers any new services or systems under the Technology Refresh Projects detailed in Schedule 16, or through any additional projects contracted through the Change Control Procedures, such new services and systems will be PSN compliant. Where any non-compliances exist in respect of the existing System that are not being resolved through the Technology Refresh Projects, the AUTHORITY will manage the risk with the PSN Authority.

## 5. ISMS

**5.1** Within 20 Working Days of the Commencement Date the PROVIDER shall review the security procedures and documentation in place under the Previous Contract and identify and submit to the AUTHORITY for the AUTHORITY's agreement any updates to the information security management system required for the purposes of this Agreement, which:

5.1.2 Not Used;

5.1.3 shall comply with the requirements of paragraphs 5.3 to 5.5 of this Schedule 7 (Security).

**5.2** The PROVIDER acknowledges that the AUTHORITY places great emphasis on the confidentiality, integrity and availability of information and consequently on the security provided by the ISMS and that the PROVIDER shall be responsible for the effective performance of the ISMS.

**5.3** The ISMS shall:

5.3.1 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's Premises, the Locations, the System (to the extent that it is under the control of the PROVIDER) and any ICT, information and data (including the AUTHORITY's Confidential Information and the AUTHORITY's Data) to the extent used by the AUTHORITY or the PROVIDER in connection with this Agreement;

5.3.2 meet the relevant standards in ISO/IEC 27001 and ISO/IEC 27002 in accordance with Paragraph 10; and

5.3.3 at all times provide a level of security which:

a) is in accordance with Good Industry Practice, law and this Agreement;

b) complies with the Baseline Security Requirements;

c) complies with the Security Policy Framework;

d) complies with at least the minimum set of security measures and standards as determined by the Security Policy Framework (Tiers 1-4);

e) meets any specific security threats to the ISMS, the Services and/or AUTHORITY Data;

f) addresses issues of incompatibility with the PROVIDER's own organisational security policies;

g) complies with ISO/IEC27001 and ISO/IEC27002 in accordance with paragraph 10; and

h) complies with the AUTHORITY's ICT and Information Assurance policies as listed in Section 13.

5.3.4 document the security incident management processes and incident response plans;

5.3.5 document the vulnerability management policy including processes for identification of system vulnerabilities and assessment of the potential impact on the Services of any new

threat, vulnerability or exploitation technique of which the PROVIDER becomes aware, prioritisation of security patches, testing of security patches, application of security patches, a process for AUTHORITY approvals of exceptions, and the reporting and audit mechanism detailing the efficacy of the patching policy; and

5.3.6 be certified by (or by a person with the direct delegated authority of) a PROVIDER's main board representative, being the Chief Security Officer, Chief Information Officer, Chief Technical Officer or Chief Financial Officer (or equivalent as agreed in writing by the AUTHORITY in advance of issue of the relevant Security Management Plan).

**5.4** Subject to Clause 47 of this Agreement (Security) the references to standards, guidance and policies set out in paragraph 5.3 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 PROVIDER from time to time.

**5.5** In the event that the PROVIDER becomes aware of any inconsistency in the provisions of the standards, guidance and policies set out in paragraph 5.3 of this Schedule, the PROVIDER shall immediately notify the AUTHORITY of such inconsistency and the AUTHORITY shall, as soon as practicable, notify the PROVIDER as to which provision the PROVIDER shall comply with.

**5.6** If the updates to the ISMS submitted to the AUTHORITY pursuant to paragraph 5.1 of this Schedule are agreed by the AUTHORITY, the revised ISMS shall be adopted by the PROVIDER immediately and thereafter operated and maintained in accordance with this Schedule. If the updates to the ISMS are not agreed by the AUTHORITY, the PROVIDER shall amend it within ten (10) Working Days of a notice of non-approval from the AUTHORITY and re-submit it to the AUTHORITY for agreement. The Parties shall use all reasonable endeavours to ensure that the agreement 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 the first revision of the ISMS to the AUTHORITY. If the AUTHORITY does not agree the ISMS following its resubmission, the matter shall be resolved in accordance with the dispute resolution procedure detailed at Clause 41. No agreement to be given by the AUTHORITY pursuant to this paragraph 5.6 of this Schedule may be unreasonably withheld or delayed. However any failure to approve the ISMS on the grounds that it does not comply with any of the requirements set out in paragraphs 5.3 to 5.5 of this Schedule shall be deemed to be reasonable.

**5.7** Agreement by the AUTHORITY of the ISMS pursuant to paragraph 5.6 of this Schedule or of any change or amendment to the ISMS shall not relieve the PROVIDER of its obligations under this Schedule.

## 6. SECURITY MANAGEMENT PLAN

**6.1** Within twenty (20) Working Days after the Commencement Date, the PROVIDER shall review and, if necessary, update the Security Management Plan created and maintained under the Previous Contract. Once updated, the PROVIDER shall submit to the AUTHORITY for agreement the fully

developed, complete and up-to-date Security Management Plan which shall comply with the requirements of paragraph 6.2 of this Schedule.

**6.2** The Security Management Plan shall:

6.2.1 be based on the initial Security Management Plan as provided under the Previous Contract;

6.2.2 comply with the Baseline Security Requirements and Security Policy;

6.2.3 identify the necessary delegated organisational roles defined for those responsible for ensuring this Schedule 7 is complied with by the PROVIDER;

6.2.4 detail the process for 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 Locations, the PROVIDER System, the AUTHORITY System (to the extent that it is under the control of the PROVIDER) and any ICT, information and data (including the AUTHORITY Confidential Information and AUTHORITY Data) and any system that could directly or indirectly have an impact on that information, data and/or Services;

6.2.5 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 Locations, the System (to the extent that it is under the control of the PROVIDER) and any ICT, information and data (including the AUTHORITY's Confidential Information and the AUTHORITY's Data) to the extent used by the AUTHORITY or the PROVIDER in connection with this Agreement;

6.2.6 set out the security measures to be implemented and maintained by the PROVIDER 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 7 (including the requirements set out in paragraph 6.2 of this Schedule);

6.2.7 demonstrate that the PROVIDER's approach to delivery of the Services has minimised the AUTHORITY and PROVIDER effort required to comply with this Schedule through consideration of available, appropriate and practicable pan-government accredited services (for example, 'platform as a service' offering from the G-Cloud catalogue);

6.2.8 set out the plans for transitioning all security arrangements and responsibilities from those in place at the Commencement Date to those incorporated in the ISMS in order for the PROVIDER to meet the full obligations of the baseline security requirements set out in Annex 1 to this Schedule 7;

6.2.9 set out the scope of the AUTHORITY System that is under the control of the PROVIDER;

6.2.10 be structured in accordance with ISO/IEC27001 and ISO/IEC27002, cross-referencing if necessary to other Schedules which cover specific areas included within those standards; and

6.2.11 be written in plain English in language which is readily comprehensible to the staff of the PROVIDER and the AUTHORITY engaged in the Services and shall reference only documents which are in the possession of the AUTHORITY or whose location is otherwise specified in this Schedule 7.

**6.3** If the updated Security Management Plan submitted to the AUTHORITY pursuant to paragraph 6.1 of this Schedule is agreed by the AUTHORITY, it shall be adopted by the PROVIDER immediately and thereafter operated and maintained in accordance with this Schedule. If the updated Security Management Plan is not agreed by the AUTHORITY, the PROVIDER shall amend it within ten (10) Working Days of a notice of non-approval from the AUTHORITY and re-submit it to the AUTHORITY for agreement. The Parties shall use all reasonable endeavours to ensure that the agreement 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 the first submission to the AUTHORITY of the updated Security Management Plan. If the AUTHORITY does not agree the Security Management Plan following its resubmission, the matter shall be resolved in accordance with the dispute resolution procedure detailed at Clause 41. No agreement to be given by the AUTHORITY pursuant to this paragraph 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 6.2 of this Schedule shall be deemed to be reasonable.

**6.4** Approval by the AUTHORITY of the Security Management Plan pursuant to paragraph 6.3 of this Schedule or of any change or amendment to the Security Management Plan shall not relieve the PROVIDER of its obligations under this Schedule.

## 7. AMENDMENT AND REVISION OF THE ISMS AND SECURITY MANAGEMENT PLAN

**7.1** The ISMS and Security Management Plan shall be fully reviewed and updated by the PROVIDER from time to time and at least annually to reflect:

7.1.1 emerging changes in Good Industry Practice;

7.1.2 any change or proposed change to the PROVIDER System, the Services and/or associated processes;

7.1.3 any new perceived or changed security threats; and

7.1.4 any reasonable request by the AUTHORITY.

**7.2** The PROVIDER shall provide the AUTHORITY with the results of such reviews as soon as reasonably practicable after their completion and amend the ISMS and Security Management Plan at no additional cost to the AUTHORITY. The results of the review shall include, without limitation:

7.2.1 suggested improvements to the effectiveness of the ISMS;

7.2.2 updates to the risk assessments;

7.2.3 maintenance of effective risk management processes including risk registers and risk treatment plans;

7.2.4 proposed modifications to the procedures and controls that effect information security to respond to events that may impact on the ISMS; and

7.2.5 suggested improvements in measuring the effectiveness of controls.

**7.3** Subject to paragraph 7.4 of this Schedule, any change or amendment which the PROVIDER proposes to make to the ISMS or Security Management Plan (as a result of a review carried out pursuant to paragraph 7.1 of this Schedule, an AUTHORITY request, change to Annex 1 (Security) or otherwise) shall be subject to the Change Control Procedures and shall not be implemented until agreed in writing by the AUTHORITY.

**7.4** The AUTHORITY may, where it is reasonable to do so, agree and require changes or amendments to the ISMS or Security Management Plan to be implemented on timescales faster than set out in the Change Control Procedures but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Change Control Procedures for the purposes of formalising and documenting the relevant change or amendment for the purposes of this Agreement.

## 8. TESTING OF THE ISMS

**8.1** The PROVIDER shall conduct tests of the ISMS ("**Security Tests**") from time to time and at least annually and additionally after any change or amendment to the ISMS or the Security Management Plan. Security Tests shall be designed and implemented by the PROVIDER so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the AUTHORITY. Subject to compliance by the PROVIDER with the foregoing requirements, if any Security Tests adversely affect the PROVIDER's ability to deliver the Services so as to meet the Service Level Performance Measures, the PROVIDER shall be granted relief against any resultant under-performance for the period of the Security Tests.

**8.2** The AUTHORITY shall be entitled to send a representative to witness the conduct of the Security Tests. The PROVIDER shall provide the AUTHORITY with the results of such Security Tests (in a form approved by the AUTHORITY in advance) as soon as practicable after completion of each Security Test.

**8.3** Without prejudice to any other right of audit or access granted to the AUTHORITY pursuant to this Agreement, the AUTHORITY and/or its authorised representatives shall be entitled, at any time and without giving notice to the PROVIDER, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the PROVIDER's compliance with the ISMS and the Security Management Plan. The AUTHORITY may notify the PROVIDER of the results of such tests after completion of each such test. If any such AUTHORITY test adversely affects the PROVIDER's ability to deliver the Services so as to meet the Service Level Performance Measures, the PROVIDER shall be granted relief against any resultant under-performance for the period of the AUTHORITY test.

**8.4** Where any Security Test carried out pursuant to paragraphs 8.2 or 8.3 of this Schedule reveals any actual or potential Breach of Security, the PROVIDER shall promptly notify the AUTHORITY of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the PROVIDER proposes to make in order to correct such failure or weakness. Subject to the AUTHORITY's prior written approval, the PROVIDER shall implement such changes to the ISMS and the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the AUTHORITY or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan is to address a non-compliance with the Security Policy or security requirements (as set out in Annex 1 to this Schedule) or the requirements of this Schedule, the change to the ISMS or Security Management Plan shall be at no cost to the AUTHORITY.

**8.5** If any repeat Security Test carried out pursuant to paragraph 8.4 of this Schedule reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall constitute a material Default of this Agreement.

## 9. IT HEALTH CHECK (ITHC)

**9.1** The parties acknowledge that IT Health Checks will be carried out on the Systems and Equipment which are used to provide the Services annually or when a condition or trigger specified in the RMADS occurs to support the accreditation process.

**9.2** IT Health Checks will be funded and initiated by the PROVIDER and carried out by a CHECK accredited organisation agreed in conjunction with the AUTHORITY. The PROVIDER has allocated thirty (30) man-days of IT Health Checks per annum.

**9.3** The AUTHORITY shall have the right to conduct its own ITHC of the PROVIDER’s system subject to twenty (20) Working Days written notice from the AUTHORITY to the PROVIDER. The frequency, scope and methods used to conduct the security assessment shall be communicated to the PROVIDER fifteen (15) Working Days prior to commencement of the ITHC. This additional ITHC will be subject to agreement via the Change Control Procedures and will be at the AUTHORITY’s cost.

**9.4** The AUTHORITY shall use its reasonable endeavours to ensure that any IT Health Checks it performs are done so in such a way as to cause as little disruption as reasonably possible to the performance of the Services and the PROVIDER’s other business.

**9.5** The AUTHORITY shall remain responsible for the remediation of all systems and services that are outside the scope of the Services (specifically those to which the PROVIDER’s system interfaces. The PROVIDER shall remain responsible for the remediation of the systems and services that are within the scope of the Services.

## 10. COMPLIANCE OF THE ISMS WITH ISO/IEC 27001 AND ISO/IEC 27002

**10.1** The AUTHORITY shall be entitled to carry out such security audits as it may reasonably deem necessary in order to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001 and ISO/IEC 27002.

**10.2** If, on the basis of evidence provided by such security audits, it is the AUTHORITY's reasonable opinion that compliance with the principles and practices of ISO/IEC 27001 or ISO/IEC 27002 is not being achieved by the PROVIDER, then the AUTHORITY shall notify the PROVIDER of the same and give the PROVIDER a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to become compliant with the principles and practices of ISO/IEC 27001 and ISO/IEC 27002. If the PROVIDER does not become compliant within the required time then the AUTHORITY shall have the right to obtain an independent audit against these standards in whole or in part.

**10.3** If, as a result of any such independent audit as described in paragraph 10.2 of this Schedule the PROVIDER is found to be non-compliant with the principles and practices of ISO/IEC 27001 or ISO/IEC 27002 then the PROVIDER 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 AUTHORITY in obtaining such audit.

## 11. BREACH OF SECURITY

**11.1** Either Party shall notify the other in accordance with the agreed security incident management process as defined by the ISMS upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.

**11.2** Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in paragraph 11.1 of this Schedule, the PROVIDER shall:

11.2.1 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 or any potential or attempted Breach of Security or protect the integrity of the ISMS against any such Breach of Security or any potential or attempted Breach of Security;

c) apply a tested mitigation against any such Breach of Security or attempted Breach of Security and, provided that reasonable testing has been undertaken by the PROVIDER, if the mitigation adversely affects the PROVIDER's ability to deliver the Services so as to meet the Performance Measures, the PROVIDER shall be granted relief against any resultant under-performance for such period as the AUTHORITY, acting reasonably, may specify by written notice to the PROVIDER;

d) prevent a further Breach of Security or any potential or attempted Breach of Security in the future exploiting the same root cause failure;

e) supply any requested data 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); and

11.2.2 as soon as reasonably practicable provide to the AUTHORITY full details (using such reporting mechanism as defined by the ISMS) of the Breach of Security or the potential or attempted Breach of Security, including a root cause analysis where required by the AUTHORITY.

**11.3** 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 ISMS with the Security Policy or Baseline Security Requirements or the requirements of this Schedule, then any required change to the ISMS shall be at no cost to the AUTHORITY.

## 12. VULNERABILITES AND CORRECTIVE ACTION

**12.1** The AUTHORITY and the PROVIDER acknowledge that from time to time vulnerabilities in the System will be discovered which unless mitigated will present an unacceptable risk to the AUTHORITY's information.

**12.2** The severity of threat vulnerabilities for PROVIDER COTS Software and Third Party COTS Software shall be categorised by the PROVIDER as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the agreed method in the ISMS and using the appropriate vulnerability scoring systems including:

12.2.1 the 'National Vulnerability Database' 'Vulnerability Severity Ratings': 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS scores as set out by NIST http://nvd.nist.gov/cvss.cfm); and

12.2.2 Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.

**12.3** The PROVIDER shall procure the application of security patches to vulnerabilities within a maximum period from the public release of such patches with those vulnerabilities categorised as 'Critical' within ten (10) Working Days of release, 'Important' within twenty-five (25) Working Days of release and all 'Other' within sixty (60) Working Days of release, except where:

12.3.1 the PROVIDER can demonstrate that a vulnerability is not exploitable within the context of any Service (e.g. because it resides in a software component which is not running in the service) provided vulnerabilities which the PROVIDER asserts cannot be exploited within the context of a Service must be remedied by the PROVIDER within the above timescales if the vulnerability becomes exploitable within the context of the Service;

12.3.2 the application of a 'Critical' or 'Important' security patch adversely affects the PROVIDER's ability to deliver the Services in which case the PROVIDER shall be granted an extension to such timescales of five (5) Working Days, provided the PROVIDER had followed and continues to follow the security patch test plan agreed with the AUTHORITY; or

12.3.3 the AUTHORITY agrees a different maximum period after a case-by-case consultation with the PROVIDER under the processes defined in the ISMS.

**12.4** The PROVIDER shall:

12.4.1 implement a mechanism for receiving, analysing and acting upon threat information supplied by GovCertUK, or any other competent Central Government Body;

12.4.2 ensure that the System (to the extent that the System is within the control of the PROVIDER) is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

12.4.3 ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the System by actively monitoring the threat landscape during the Agreement Period;

12.4.4 pro-actively scan the System (to the extent that the System is within the control of the PROVIDER) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS;

12.4.5 from the date specified in the Security Management Plan provide a report to the AUTHORITY within five (5) Working Days of the end of each month detailing both patched and outstanding vulnerabilities in the System (to the extent that the System is within the control of the PROVIDER) and any elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report;

12.4.6 propose interim mitigation measures to vulnerabilities in the System known to be exploitable where a security patch is not immediately available;

12.4.7 remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the System); and

12.4.8 inform the AUTHORITY when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the System and provide initial indications of possible mitigations.

**12.5** If the PROVIDER is unlikely to be able to mitigate the vulnerability within the timescales under this Paragraph 12, the PROVIDER shall immediately notify the AUTHORITY.

**12.6** A failure to comply with Paragraph 12.3 shall require the PROVIDER to provide a rectification plan within ten (10) Working Days of becoming aware of such non-compliance.

## 13. ICT AND INFORMATION ASSURANCE POLICIES

**13.1** Subject to paragraphs 13.3. and 13.4 below, the PROVIDER will use reasonable endeavours to comply with the AUTHORITY's ICT and Information Assurance policies to be provided to it within thirty (30) days of the Commencement Date.

**13.2** The AUTHORITY will provide the AUTHORITY's updated ICT and Information Assurance Policies on an annual basis to the PROVIDER.

**13.3** Where the PROVIDER cannot comply with the AUTHORITY's ICT or Information Assurance Policies (or any updates to them), the PROVIDER will notify the AUTHORITY of the reason why within ten (10) Working Days of receipt of the ICT and Information Assurance Policies (or any updates to them).

**13.4** Where the AUTHORITY has provided an ICT or Information Assurance Policy (or any updates to them) that cannot be complied with unless a change is made to the Services that the PROVIDER delivers, then this will be subject to the Change Control Procedures.

## ANNEX 1: BASELINE SECURITY REQUIREMENTS

### 1. HIGHER CLASSIFICATIONS

**1.1** The PROVIDER shall not handle AUTHORITY information classified SECRET or TOP SECRET except if there is a specific requirement and in this case prior to receipt of such information the PROVIDER shall seek additional specific guidance from the AUTHORITY.

### 2. VISOR SECURITY CONTROLS

**2.1** The PROVIDER will implement the ViSOR security controls as defined in Annex 2 to this Schedule 7.

### 3. END USER DEVICES

**3.1** 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 the AUTHORITY's accreditation process.

### 4. DATA PROCESSING, STORAGE, MANAGEMENT AND DESTRUCTION

**4.1** The PROVIDER and AUTHORITY recognise the need for the AUTHORITY's information to be safeguarded under Data Protection Legislation or a similar regime. To that end, the PROVIDER 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 Data will be subject to at all times.

**4.2** The PROVIDER 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. Such approval shall not be unreasonably withheld or delayed unless specified otherwise in this Agreement and provided that storage, processing and management of any AUTHORITY Data is only carried out offshore within:

4.2.1 the European Economic Area (EEA);

4.2.3 in the US if the PROVIDER and or any relevant Sub-contractor have signed up to the US-EU Safe Harbour Agreement; or

4.2.4 in another country or territory outside the EEA if that country or territory ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into which have been defined as adequate by the EU Commission.

**4.3** The PROVIDER shall:

4.3.1 provide the AUTHORITY with all AUTHORITY Data on demand in an agreed open format;

4.3.2 have documented processes to guarantee availability of AUTHORITY Data in the event of the PROVIDER ceasing to trade;

4.3.3 dispose of all Assets and securely destroy all media that has held AUTHORITY Data at the end of life of that media in line with

Information Assurance Standard 5 (IAS5) as further detailed in Schedule 3 (PROVIDER's Solution) paragraph 27; and

4.3.4 securely erase any or all AUTHORITY Data held by the PROVIDER when requested to do so by the AUTHORITY in line with IAS5.

## 5. NETWORKING

**5.1** 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).

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

## 6. SECURITY ARCHITECTURES

**6.1** The PROVIDER 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 Data.

**6.2** When designing and configuring the System (to the extent that the System is within the control of the PROVIDER) the PROVIDER shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or a CESG Certified Professional certification (http://www.cesg.gov.uk/awarenesstraining/IA-certification/Pages/index.aspx) for all bespoke or complex components of the System (to the extent that the System is within the control of the PROVIDER).

## 7. PERSONNEL SECURITY

**7.1** PROVIDER Personnel shall be subject to pre-employment checks that include, as a minimum: identity, unspent criminal convictions and right to work.

**7.2** The PROVIDER shall agree on a case by case basis PROVIDER 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.

**7.3** The PROVIDER shall prevent PROVIDER 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.

**7.4** All PROVIDER 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.

**7.5** Where the PROVIDER or Sub-Contractors grants increased ICT privileges or access rights to PROVIDER Personnel, those PROVIDER 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 one (1) Working Day.

## 8. IDENTITY, AUTHENTICATION AND ACCESS CONTROL

**8.1** The PROVIDER shall operate an access control regime to ensure all users and administrators of the System (to the extent that the System is within the control of the PROVIDER) 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 System that they require. The PROVIDER shall retain an audit record of accesses.

## 9. AUDIT AND MONITORING

**9.1** The PROVIDER 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 PROVIDER audit records should (as a minimum) include:

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

9.1.2 Security events generated in the System (to the extent that the System is within the control of the PROVIDER) 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.

**9.2** The PROVIDER and the AUTHORITY shall work together to establish any additional audit and monitoring requirements for the System.

**9.3** The PROVIDER shall retain audit records collected in compliance with this Paragraph 9 for a period of at least six (6) months.

## ANNEX 2: VISOR SECURITY CONTROLS [REDACTED]