Schedule 2.4 – ESMCP Mobile Services Agreement

Security Management

Version 1.0

CHANGE HISTORY

Version No.	Effective Date / agreement / CAN	Version / Details of Changes included in Update	Author(s)
1.0	01/12/2024	Execution version	ESMCP

Contents

1 Definitions

1.1 In construing this Schedule 2.4 (Security Management), unless otherwise expressly specified in this Schedule terms defined and used in Schedule 1 (Definitions) will have the same meaning in this Schedule.

1.2 For the purposes of this Schedule 2.4 (Security Management) only the term “ESN Specific Network Element” means those components (including, without limitation, any software, systems, processes, assets, or ESN Products) that the Supplier has deployed exclusively in support of the ESN Services.

2 Introduction

2.1 The Parties acknowledge that the purpose of the ISMS and 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 Parties shall each appoint a member of the Technical Design Authority to be responsible for security. The initial member of the Technical Design Authority appointed by the Supplier for such purpose shall be the person named as such in Schedule 9.2 (Key Personnel) and the provisions of Clauses 14.5 and 14.6 (Key Personnel) shall apply in relation to such person.

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

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

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

3 Information Security Management System (ISMS)

3.1 Within twenty one (21) months after the Effective Date, the Supplier shall develop and submit to the Authority, for the Authority's approval in accordance with Paragraph 3.6, an ISMS for the purposes of this Agreement, which:

(a) shall have been tested in accordance with Schedule 6.2 (Testing and Assurance Procedures); and

(b) shall comply with the requirements of Paragraphs 3.3 to 3.5.

3.2 The Supplier acknowledges that the Authority places great emphasis on the reliability of the services for confidentiality, integrity, availability, and authenticity of information and consequently on the security, non-repudiation and accountability provided by the ISMS and that it shall be responsible for the effective performance of the ISMS.

3.3 The ISMS shall:

(a) 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 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;

(b) meet the requirements of the ISO/IEC 27001 and ISO/IEC 27002 standards in accordance with Paragraph 7;

(c) at all times provide a level of security which:

(i) is in accordance with Law and this Agreement;

(ii) as a minimum demonstrates Good Industry Practice;

(iii) complies with the Baseline Security Requirements;

(iv) addresses issues of incompatibility with the Supplier's own organisational security policies;

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

(vi) supports compliance with the requirements set out in the Security Policy Framework and other government and NCSC guidance;

(vii) complies with the security requirements as set out in Schedule 2.1 (Service Description);

(d) document the security incident management processes and incident response plans in sufficient detail to the extent to which planned activities are realised and planned results achieved to ensure it is fit for purpose and enables the recovery of services to be achieved with minimum resources, effort and costs;

(e) document the vulnerability management policy and assessment of the potential impact on the Services of any new threat, vulnerability or exploitation technique of which the Supplier becomes aware; and

(f) be certified by (or by a person with the direct delegated authority of) a Supplier'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).

3.4 Subject to Clause 19.11 (Authority Data and Security Requirements) the references to standards, guidance and policies set out in Paragraph 3.3 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 identified by or notified to the Supplier from time to time.

3.5 In the event that the Supplier becomes aware of any inconsistency in the provisions of the standards, guidance and policies set out in Paragraph 3.3, the Supplier shall immediately notify the Authority Representative of such inconsistency and the Authority Representative shall, as soon as practicable, notify the Supplier which provision the Supplier shall comply with.

3.6 If the ISMS submitted to the Authority pursuant to Paragraph 3.1 is approved by the Authority, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the ISMS is not approved by the Authority, the Supplier shall amend it within [redacted] of a notice of non-approval from the Authority and re-submit it to the Authority 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 [redacted] (or such other period as the Parties may agree in writing) from the date of its first submission to the Authority. If the Authority does not approve the ISMS following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Authority pursuant to this Paragraph 3 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 3.3 to 3.5 shall be deemed to be reasonable.

3.7 Approval by the Authority of the ISMS pursuant to Paragraph 3.6 or of any change or amendment to the ISMS shall not relieve the Supplier of its obligations under this Schedule.

4 Security Management Plan

4.1 Within [redacted] after the Effective Date, the Supplier shall prepare and submit to the Authority for approval in accordance with Paragraph 4.4 a fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of Paragraph 4.3.

4.2 Within [redacted] after the Effective Date, the Supplier shall prepare and submit to the Authority a formal Risk Assessment and a Risk Treatment Plan for the scope of the ISMS and a risk treatment plan for the scope of the ISMS which informs and supports updates to the Security Management Plan. This Risk Assessment shall be based on a risk framework and methodology identified by the Supplier and subsequently approved by the Authority and describe the current threat landscape, the security risks to ESN and the security measures and mitigations in place.

4.3 The Security Management Plan shall:

(a) be based on the Security Management Plan set out in Annex 2, which is the most recent version of the Security Management Plan that has been approved by the Authority;

(b) comply with the Baseline Security Requirements;

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

(d) detail the process for managing any security risks from Sub-contractors (including ensuring the provision of a Security Aspects Letter and, where relevant, regarding the inclusion or exclusion of relevant terms in the Sub-contract, as identified in Schedule 4.3 (Notified Key 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;

(e) 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;

(f) 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 (including the requirements set out in Paragraph 3.3);

(g) demonstrate that the Supplier Solution has minimised the Authority and Supplier effort required to comply with this Schedule through consideration of available, appropriate and practicable pan-government accredited services;

(h) set out the plans for transiting all security arrangements and responsibilities from those in place at the Effective Date to those incorporated in the Supplier submitted ISMS and for the Supplier to meet the full obligations of the security requirements set out in Schedule 2.1 (Services Description) and this Schedule;

(i) set out the scope of the Authority System that is under the control of the Supplier;

(j) 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;

(k) 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; and

(l) be Protectively Marked in accordance with the Cabinet Office Government Security Classification Policy and the Security Policy Framework.

4.4 If the Security Management Plan submitted to the Authority pursuant to Paragraph 4.1 is approved by the Authority, 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, the Supplier shall amend it within [redacted] of a notice of non-approval from the Authority and re-submit it to the Authority 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 [redacted] (or such other period as the Parties may agree in writing) 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 shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Authority pursuant to this Paragraph 4.4 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 4.3 shall be deemed to be reasonable.

4.5 Approval by the Authority of the Security Management Plan pursuant to Paragraph 4.4 or of any change or amendment to the Security Management Plan shall not relieve the Supplier of its obligations under this Schedule.

5 Amendment And Revision Of The ISMS, Security Management Plan & Risk Assessment

5.1 The ISMS, Security Management Plan and Risk Assessment shall be fully reviewed and updated by the Supplier from time to time and at least annually to reflect:

(a) emerging changes in Good Industry Practice or relevant industry standards;

(b) any change or proposed change to the IT Environment, the Services and/or associated processes, including any changes which are brought about by the provision of 5G capability;

(c) The security measures and activities which the Supplier has implemented, or proposes to implement, into the ESN Specific Network Elements which are the same or substantially similar to the security measures and activities that the Supplier has implemented, or proposes to implement, into the Supplier's commercial network in order to achieve compliance with the Telecommunications Security Act (TSA) 2021;

(d) any new perceived or changed security threats;

(e) any change or proposed change to the Security Policy Framework;

(f) any change or proposed change to the NCSC/NPSA guidance; and

(g) any reasonable change in requirement requested by the Authority.

5.2 The Supplier shall provide the Authority with the results of each review of the ISMS, Security Management Plan and Risk Assessment as soon as reasonably practicable after their completion and amend the ISMS, Security Management Plan and Risk Assessment at no additional cost to the Authority. The results of the Security Management Plan review shall include, without limitation:

(a) suggested improvements to the effectiveness of the ISMS;

(b) updates to the Risk Assessments;

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

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

5.3 Subject to Paragraph 5.5, any change or amendment which the Supplier proposes to make to the ISMS or Security Management Plan (as a result of a review carried out pursuant to Paragraph 5.1, an Authority change to Schedule 2.1 (Services Description) or otherwise) shall be subject to the Change Control Procedure and shall not be implemented until approved in writing by the Authority.

5.4 The Supplier will implement the security measures referred to in Paragraph 5.1(c) above automatically where possible and any change or amendment to those measures will also be implemented automatically where possible.

5.5 The Authority may at any time, whether prior to or after implementation of the security measures or activities referred to in Paragraph 5.1(c), request a change to the ESN Specific Network Element which shall be subject to the Change Control Procedure.

5.6 The Authority may, where it is reasonable to do so, approve 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 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 for the purposes of this Agreement.

5.7 If any review required by Paragraph 5.1 identifies any issues of non compliance with the requirements of Schedule 2.4, or results in changes to the Risk Assessment, including the introduction of new risks or increase in existing risk levels which are;

5.7.1 due to changes in the Supplier's infrastructure, technology, supply chain, processes or organisation; or

5.7.2 due to changes to the threat landscape which affect the Supplier and/or BT Group as a whole;

then it will be the Supplier's responsibility to put appropriate controls in place to manage such risks. If any such changes to the Risk Assessment are as a result of changes to the threat landscape that are exclusively concerned with ESN and which would not otherwise impact the Supplier, or as a result of new or changed Authority Requirements then the introduction or enhancement of appropriate controls shall be addressed by a Change Request.

5.8 The Supplier will discuss TSA compliance measures with the Authority and will have regard to any suggestions the Authority makes, but notwithstanding any term to the contrary in this Schedule 2.4, the Supplier is solely responsible for TSA compliance and the measures the Supplier at its discretion chooses to implement to the Supplier's commercial network.

6 Security Testing

6.1 The Supplier shall, at its own cost and expense procure and conduct:

6.1.1 testing of the ISMS by a CHECK Service Provider ("IT Health Check");

6.1.2 relevant Security Tests which are:

(a) from time to time and at least annually across the scope of the ISMS;

(b) after significant architectural changes to the IT Environment;

(c) after any change or amendment to the ISMS, (including security incident management processes and incident response plans) or the Security Management Plan; and

(d) such other security tests as requested by the Authority and agreed in good faith to be reasonable. If the Parties cannot agree in good faith what is to be regarded as reasonable in the circumstances, the matter shall be resolved in accordance with the Dispute Resolution Procedure.

6.2 NOT USED.

6.3 The output of such Security Tests should be recorded in a format agreed by the Authority.

6.4 Within [redacted] after the Effective Date the Supplier shall prepare and submit to the Authority for approval a template to be used for reporting Security Test results (the "Security Test Results Template").

6.5 If the Security Test Results Template submitted to the Authority pursuant to Paragraph 6.4 is approved by the Authority, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Test Results Template is not approved by the Authority, the Supplier shall amend it within [redacted] Days of a notice of non-approval from the Authority and re-submit it to the Authority 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 [redacted] (or such other period as the Parties may agree in writing) from the date of its first submission to the Authority. If the Authority does not approve the Security Test Results Template following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Authority pursuant to this Paragraph 6.5 may be unreasonably withheld or delayed. However any failure to approve the Security Test Results Template on the grounds that it does not comply with the requirements set out in Paragraph 6.1 shall be deemed to be reasonable.

6.6 The Supplier shall submit to the Authority the output of all Security Tests carried out in accordance with Schedule 6.1 (Implementation Plan), using the Security Test Results Template approved by the Authority within no more than [redacted] (or such other period as the Parties may agree in writing) from the date of completion of the relevant Security Test.

6.7 The Authority shall be entitled to send representation to witness the conduct of Security Tests.

6.8 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 upon giving reasonable notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the Supplier's compliance with the ISMS and the Security Management Plan. The Authority may notify the Supplier of the results of such tests after completion of each such test. If any such Authority test adversely affects the Supplier's ability to deliver the Services so as to meet the Minimum

Service Thresholds, the Supplier shall be granted relief against any resultant under-performance for the period of the Authority test.

6.9 Subject to Paragraph 6.10, the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Authority. Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier's ability to deliver the Services so as to meet the Minimum Service Thresholds, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests.

6.10 The Supplier agrees that the Authority is able to request Security Tests without prior notice.

6.11 In relation to each IT Health Check, the Supplier shall:

6.11.1 agree with the Authority the aim and scope of the IT Health Check;

6.11.2 promptly, and no later than [redacted] following the receipt of each IT Health Check report, provide the Authority with a copy of the full report;

6.11.3 in the event that the IT Health Check report identifies any vulnerabilities, the Supplier shall:

(a) prepare a remedial plan for approval by the Authority (each a "Remediation Action Plan") which sets out in respect of each vulnerability identified in the IT Health Check report:

(b) how the vulnerability will be remedied;

(c) unless otherwise agreed in writing between the Parties, the date by which the vulnerability will be remedied, which must be:

(d) within [redacted] of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of "medium";

(e) within thirty (30) days of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of "high", including vulnerabilities affecting externally exposed interfaces, and within ninety (90) days for vulnerabilities affecting internally exposed interfaces; and

(f) within [redacted] of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of "critical", including vulnerabilities affecting externally exposed interfaces, and within [redacted] for vulnerabilities affecting internally exposed interfaces;

(g) the tests which the Supplier shall perform or procure to be performed (which may, at the discretion of the Authority, include a further IT Health Check) to confirm that the vulnerability has been remedied;

(h) comply with the Remediation Action Plan; and

(i) conduct such further tests on the Service as are required by the Remediation Action Plan to confirm that the Remediation Action Plan has been complied with.

6.12 The Supplier shall ensure that any testing which could adversely affect the Supplier System shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such tests shall be agreed in advance with the Authority.

6.13 If any testing conducted by or on behalf of the Supplier identifies a new risk, new threat, vulnerability or exploitation technique, or any actual or potential Breach of Security or weaknesses (included un-patched vulnerabilities, poor configuration and/or incorrect system management) that has the potential to materially diminish the effectiveness of the ISMS, the Supplier shall within [redacted] of becoming aware of such findings provide the Authority with a copy of the test report and:

(a) notify the Authority of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such findings;

(b) propose interim mitigation measures to vulnerabilities in the ISMS known to be exploitable where a security patch is not immediately available; and

(c) where and to the extent applicable, 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 Supplier System) within the timescales set out in the test report or such other timescales as may be agreed with the Authority.

6.14 Subject to the Authority's prior written approval, the Supplier 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.

6.15 Where the change to the ISMS or Security Management Plan is to address a non-compliance with the Baseline Security Requirements or security requirements (as set out in Schedule 2.1 (Services Description)) or the requirements of this Schedule, the change to the ISMS or Security Management Plan shall be at no cost to the Authority.

6.16 NOT USED.

6.17 The Supplier shall notify the Authority immediately if it fails to, or believes that it will not, mitigate the vulnerability within the timescales set out in Paragraph 6.11.

6.18 Security Tests should comply with the recommendations set out in the Security Policy Framework and relevant NCSC guidance.

6.19 If any repeat Security Test carried out pursuant to Paragraph 6.9 reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall constitute a material Default for the purposes of Clause 26.1(c) (Rectification Plan Process).

7 Compliance Of The ISMS with ISO/IEC 27001

7.1 Where Authority Data is stored, processed or transmitted, and under the management and/or control of the Supplier, the Supplier shall achieve and maintain ISO/IEC 27001 certification of compliance for those services, systems, processes and procedures throughout the Term of this Agreement.

7.2 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, the specific security requirements set out in Schedule 2.1 (Services Description) and the Baseline Security Requirements.

7.3 If, on the basis of evidence provided by such audits, it is the Authority's reasonable opinion that compliance with the principles and practices of ISO/IEC 27001, the specific security requirements set out in Schedule 2.1 (Services Description) and/or the Baseline Security Requirements is not being achieved by the Supplier, then the Authority shall notify the Supplier of the same and give the Supplier a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to implement any necessary remedy. If the Supplier 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.

7.4 If, as a result of any such independent audit as described in Paragraph 7.3 the Supplier is found to be non-compliant with the principles and practices of ISO/IEC 27001, the specific security requirements set out in Schedule 2.1 (Services Description) and/or the Baseline Security Requirements then the Supplier shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the Authority in obtaining such audit.

8 Breach Of Security

8.1 If a Breach of Security or attempted Breach of Security is discovered by either Party, that Party shall notify the other Party using the security incident management processes and procedures expressed and agreed in the ISMS.

8.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 8.1, 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) 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 Supplier, if the mitigation adversely affects the Supplier's ability to

deliver the Services so as to meet the Minimum Service Thresholds, the Supplier shall be granted relief against any resultant under-performance for such period as the Authority, acting reasonably, may specify by written notice to the Supplier; and

(iv) prevent a further Breach of Security or any potential or attempted Breach of Security in the future exploiting the same root cause failure.

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

8.3 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 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 ISMS shall be at no cost to the Authority.

ANNEX 1: Baseline Security Requirements

Valuation and Classifications of Assets

1 The Supplier shall evaluate and classify Authority assets using industry good practice, ensuring that access to Authority Data and other assets is correctly managed and that the physical, procedural, personnel and technical areas of the assets are safeguarded to an agreed and proportionate level throughout their lifecycle, including creating, processing, storage, transmission and destruction. The Supplier shall ensure that:

(a) the system is designed to support HMG business, and meet the requirements of relevant legislation, international standards, international agreements, and contractual obligations;

(b) the system is designed to protect information (and other assets) from accidental or deliberate compromise, which may lead to damage and/or criminal offence;

(c) operational data (as defined in the Security Aspects Letter) and information assets remain the property of the rightful User Organisation irrespective of any proprietary or open standard technique used to format or package the data;

(d) the Authority Data is only accessible to those verified with a need to know and that the location of where data is stored is transparent to the Authority and available upon request; and

(e) formal approval is sought from the Authority prior to sharing any data generated from User activity, User Device data or User identity data with any third party.

Data Processing, Storage, Management and Destruction

2 The Supplier and Authority recognise the need for the Authority Personal Data to be safeguarded under the Data Protection Legislation. To that end, the Supplier must be able to state to the Authority the physical locations in which the Authority Data/Information may be stored, processed and managed from, and what legal and regulatory frameworks Authority Data/Information will be subject to at all times.

3 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. Such approval shall not be unreasonably withheld or delayed provided that any proposed change is in accordance with the Security Policy Framework.

4 Where the Supplier stores Authority Data (that is under the management and control of the Supplier, the Supplier shall:

(a) provide the Authority within [redacted] of a request, a data sample of sufficient quantity to ascertain potential risks from compromise, loss or theft. The data shall be sent by the Supplier to the Authority in a secure format to be prescribed by the Authority, at no additional cost to the Authority;

(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 the Security Policy Framework;

(d) securely erase any or all Authority Data held by the Supplier when requested to do so by the Authority in line with the Security Policy Framework; and

(e) ensure that any Personal Data that is no longer required is securely erased in accordance with NCSC/NPSA guidance.

Networking

5 The Supplier shall ensure that the network control function (the means and mechanisms used to configure network components (routers, switches, firewalls)) remains within the physical boundaries of the UK. This shall be done in accordance with the Security Policy Framework and NCSC guidance.

6 The Supplier shall ensure that the network and service function provided is accessible and controllable from within the physical boundaries of the UK.

Personnel Security

7 Supplier Personnel shall be subject to pre-employment checks that are compliant with ISO/IEC 27001 and ISO/IEC 27002, HMG Personnel Security Controls and BPSS standard, which shall include the verification of, as a minimum: identity, employment history, unspent criminal convictions and right to work.

8 At a time agreed between the Supplier and Authority, but in any event within ninety (90) days after the Effective Date, the Supplier in collaboration with the Authority shall conduct a Personnel Security Risk Assessment for each role within their organisation where that role will have direct access to Authority information or assets. The Supplier may choose the method of assessment, but it must conform to Good Industry Practice or the most up to date version of the NPSA 'Personnel Security Risk Assessment'.

9 The Supplier shall agree with the Authority on a case by case basis those Supplier Personnel roles that require National Security Clearance such as Counter Terrorist Check (CTC), Security Check (SC) or possibly Developed Vetting (DV). These roles include, but are not limited to:

(a) the Supplier employees, contractors or Sub-contractors' system administrators; and

(b) individuals with elevated privileges that can access IT systems which store or process Authority Data.

10 The Supplier shall obtain the necessary clearance for each of its staff before services or systems are made operational whereby Authority data is stored, processed or transmitted on or over Supplier infrastructure and in any event within 21 months after the Effective Date. Any costs associated with obtaining the necessary staff clearances shall be borne by the Supplier.

11 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.

12 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.

13 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 [redacted]

Business Continuity and Disaster Recovery

14 The Supplier shall produce a Business Continuity Management System in accordance with BS ISO 22301.