# Schedule 2.4 - Lot 2

# Security Management

**Version 5.0**



This document is based on Schedule 2.4 of the Crown Commercial Services Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

**CHANGE HISTORY**

| Version No. | Date | Details of Changes included in Update | Author(s) | Document Number |
|---|---|---|---|---|
| 4.0 | 14.10.15 | Execution version | ESMCP | 35090765.19 |
| 4.1 | 08.11.18 | Updated in anticipation of CAN | DLAP | 92724887 |
| 4.2 | 23.11.18 | Updated as part of CAN 500 | Motorola | 44515639.1 |
| 4.3 | 19.12.18 | Updated in anticipation of CAN | DLAP | 92724887 |
| 4.4 | 04.01.19 | Motorola changes | Motorala/ B&B | |
| 4.5 | 17.01.19 | Updated in line with conversations | Motorala/ B&B | |
| 5.0 | 13.05.19 | CAN500 Execution version | DLAP | 96288867.1 |



This document is based on Schedule 2.4 of the Crown Commercial Services Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

# Contents


| | | |
|---|---|---|
| **1** | **Definitions** | **4** |
| **2** | **Introduction** | **4** |
| **3** | **Information Security Management System (ISMS)** | **4** |
| **4** | **Security Management Plan** | **6** |
| **5** | **Amendment And Revision Of The ISMS And Security Management Plan** | **8** |
| **6** | **Security Testing** | **9** |
| **7** | **Compliance Of The ISMS with ISO/IEC 27001** | **10** |
| **8** | **Breach Of Security** | **11** |
| **9** | **Vulnerabilities and Corrective Action** | **12** |
| **ANNEX 1: Baseline Security Requirements** | | **15** |
| **ANNEX 2: Security Management Plan** | | **22** |




This document is based on Schedule 2.4 of the Crown Commercial Services Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

## 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.

## 2 Introduction

2.1 The Parties acknowledge that the purpose of the Information Security Management System 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 Delivery Working Group to be responsible for security. The initial member of the Technical Delivery Working Group 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 the 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 4.3 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.



This document is based on Schedule 2.4 of the Crown Commercial Services Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

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 relevant standards in ISO/IEC 27001 and ISO/IEC 27002 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) complies with at least the minimum set of security measures and standards set out in the Security Policy Framework (Tiers 1-4); and

(vii) complies with the security requirements as set out in Schedule 2.1 (Services Description).

(d) define the security incident management processes, procedures 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) define the vulnerability management processes and procedures to be employed by the Supplier to identity system vulnerabilities, including an assessment of the potential impact on the Services of any new threat, vulnerability or exploitation technique of which the Supplier becomes aware of;

(f) define and implement the process and procedures for deploying security patches to include but not be limited to, prioritising, testing, approving patches, and a process for exceptions approved by the Authority, and the reporting and audit mechanism detailing the efficiency of the patching policy; and

(g) 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).



This document is based on Schedule 2.4 of the Crown Commercial Services Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

3.4 Subject to Clause 20.11 (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 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 ten (10) Working 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 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. 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 thirty (30) Working Days after the Effective Date, the Supplier shall prepare and submit to the Authority for approval in accordance with Paragraph 4.3 a fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of Paragraph 4.2.

4.2 The Security Management Plan shall:

(a) be based on the Security Management Plan set out in Annex 2 and as submitted as part of the Supplier's ITSB response;

(b) comply with the Baseline Security Requirements as set out in Annex 1;

(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 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



This document is based on Schedule 2.4 of the Crown Commercial Services Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

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 (for example, 'platform as a service' offerings from the G-Cloud catalogue);

(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 at the date set out in Schedule 6.1 (Implementation Plan) 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.

4.3 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 ten (10) Working 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 fifteen (15) Working Days (or such other



This document is based on Schedule 2.4 of the Crown Commercial Services Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

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 4.3 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 4.2 shall be deemed to be reasonable.

4.4 Approval by the Authority of the Security Management Plan pursuant to Paragraph 4.3 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 And Security Management Plan

5.1 The ISMS and Security Management Plan 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;

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

(c) any new perceived or changed security threats;

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

(e) any change or proposed change to the CESG IA Policy Portfolio; and

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

5.2 The Supplier 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 each 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 5.4, 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 request, 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.



This document is based on Schedule 2.4 of the Crown Commercial Services Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

5.4 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.

## 6 Security Testing

6.1 The Supplier shall conduct relevant Security Tests from time to time (and at least annually across the scope of the ISMS) and additionally after significant architectural changes to the IT Environment or after any change or amendment to the ISMS, (including security incident management processes and incident response plans) or the Security Management Plan. The implementation of Security Tests shall be designed by the Supplier so as to minimise the impact on the delivery of the Services. Subject to Paragraph 6.2, 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. The output of such tests should be recorded in a format agreed by the Authority.

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

6.3 Security Tests should comply with the recommendations set out in the Security Policy Framework and CESG IA Policy Portfolio.

6.4 Within thirty (30) Working Days after the Effective Date the Supplier shall prepare and submit to the Authority for approval in accordance with Paragraph 6.1, 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 ten (10) Working 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 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. 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 on the Authority System that is under the control of the Supplier, using the Security Test Results Template approved by the Authority within no more than fifteen (15) Working Days (or such other period as the Parties may agree in writing) from the date of test completion.



This document is based on Schedule 2.4 of the Crown Commercial Services Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

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 Where any Security Test carried out pursuant to Paragraphs 6.1 or 6.8 reveals any actual or potential Breach of Security or weaknesses (included un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly 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 failure or weakness. 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. 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.

6.10 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 27.1(c) (Rectification Plan Process).

## 7 Compliance Of The ISMS with ISO/IEC 27001

7.1 Where Authority Information or 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 contract.

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 Security audits can include but are not limited to HMG Accreditation as detailed in the Security Policy Framework and CESG IA Policy Portfolio, and/or the Home Office Supplier Assurance process (HADRIAN).

7.4 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



This document is based on Schedule 2.4 of the Crown Commercial Services Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

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.

7.5 If, as a result of any such independent audit as described in Paragraph 7.4 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;

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

(v) supply any requested data to the Authority or the Computer Emergency Response Team for UK Government (“GovCertUK”) or for CESG encrypted products (CINRAS) 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



This document is based on Schedule 2.4 of the Crown Commercial Services Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

(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.

## 9 Vulnerabilities and Corrective Action

9.1 The Authority and the Supplier acknowledge that from time to time vulnerabilities in the IT Environment will be discovered which unless mitigated will present an unacceptable risk to the Authority's information.

9.2 The severity of threat vulnerabilities for Supplier COTS Software and Third Party COTS Software shall be categorised by the Supplier 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:

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

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

9.3 The Supplier 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 fourteen (14) days of release, 'Important' within thirty (30) days of release and all 'Other' within sixty (60) Working Days of release, except where:

(a) the Supplier 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 Supplier asserts cannot be exploited within the context of a Service must be remedied by the Supplier within the above timescales if the vulnerability becomes exploitable within the context of the Service;

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

(c) the Authority agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the ISMS.

9.4 The Supplier Solution and Schedule 6.1 (Implementation Plan) shall include provisions for major version upgrades of all Supplier COTS Software and Third Party COTS Software to be upgraded within 6 months of the release of the latest version, such that it is no more than one



This document is based on Schedule 2.4 of the Crown Commercial Services Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

major version level below the latest release (normally codified as running software no older than the 'n-1 version') throughout the Term unless:

(a) where upgrading such Supplier COTS Software and Third Party COTS Software reduces the level of mitigations for known threats, vulnerabilities or exploitation techniques, provided always that such upgrade is made within 12 months of release of the latest version; or

(b) is agreed with the Authority in writing.

9.5 The Supplier shall:

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

(b) ensure that the IT Environment (to the extent that the IT Environment is within the control of the Supplier) is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

(c) ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the IT Environment by actively monitoring the threat landscape during the Term;

(d) pro-actively scan the IT Environment (to the extent that the IT Environment is within the control of the Supplier) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS as developed under Paragraph 3.3(e);

(e) from the date specified in the Security Management Plan (and before the first Operational Service Commencement Date) 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 IT Environment (to the extent that the IT Environment is within the control of the Supplier) 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;

(f) propose interim mitigation measures to vulnerabilities in the IT Environment known to be exploitable where a security patch is not immediately available;

(g) 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 Solution and IT Environment); and

(h) 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 IT Environment and provide initial indications of possible mitigations.

9.6 If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under this paragraph 9, the Supplier shall immediately notify the Authority.



This document is based on Schedule 2.4 of the Crown Commercial Services Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

9.7 A failure to comply with Paragraph 9.3 shall constitute a Notifiable Default, and the Supplier shall comply with the Rectification Plan Process.



This document is based on Schedule 2.4 of the Crown Commercial Services Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

## ANNEX 1: Baseline Security Requirements

### Valuation and Classifications of Assets

1 The Supplier shall adopt the Cabinet Office Government Security Classification Policy (GSCP) as an administrative system to ensure 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 and international agreements;

(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 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.

2 The level of classification must be viewed against the legal background including the requirements of the Official Secrets Acts 1911 and 1989, FOIA and DPA.

3 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 receipt of such information the Supplier shall seek additional specific guidance from the Authority.

### Information Risk Management

4 The risk assessment methodology implemented under this Agreement must align with CESG Information Assurance Standards Number 1 & 2 and its associated CESG Good Practice Guidance 47 'Information Risk Management'.

5 The Supplier shall work with the Authority to identify, assess and treat the technical risks for all HMG Information and Communication Technology (ICT) systems or services that handle, store or process protectively marked Government information or business critical data.



This document is based on Schedule 2.4 of the Crown Commercial Services Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

**Privacy Impact Assessment (PIA)**

6 Within 21 months after the Effective Date, the Supplier shall conduct a Privacy Impact Assessment ("PIA") in accordance with the guidance detailed on the Information Commissioner's Office website: http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment

7 The Authority reserves the right to see results of PIA once they are available.

**Device Management**

Except to the extent that the Authority drafted and maintained UDDS prevents the Supplier from being able to comply with the following paragraphs 8-10 ( inclusive) (and any disagreement as to whether this is the case shall be dealt with through the Dispute Resolution Procedure with automatic reference to expert determination (without mediation) under Paragraph 5 of that procedure in the event of a failure to agree a resolution of the Dispute as a result of commercial negotiations under Paragraph 3 of that procedure), the Supplier shall comply with the following User Device management security requirements:

8 Whether the User Device is being used within and/or outside of network Coverage, or being used in direct device to device mode, the Supplier shall ensure that information is not made available or disclosed to unauthorised individuals, entities or processes and that the information (voice and data) is not altered or changed in anyway whether the information is at rest or in transit.

9 When Authority Data resides on a mobile device, 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 approved by CESG (Government's National Technical Authority for Information Assurance (IA)), to at least Foundation Grade, for example, under the CESG Commercial Product Assurance scheme ("CPA") or an equivalent assurance process approved by the Authority.

10 The Supplier shall have responsibility for ensuring that only known and Authority authorised User Devices are able to connect to and utilise its systems and services. Those devices approved shall have a minimum set of security controls provisioned and enforced through policy.

11 The Supplier shall only enable access to those devices that it can determine the origin of manufacture for and which are from a known and reputable source, and that have not been modified or tampered with, without Authority approval. Unless otherwise agreed with the Authority in writing, all User 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-security). Where the guidance highlights shortcomings in a particular platform and the Supplier may wish to use alternate mechanisms, 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.



This document is based on Schedule 2.4 of the Crown Commercial Services Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

**Data Processing, Storage, Management and Destruction**

12 The Supplier and Authority recognise the need for the Authority Personal Data to be safeguarded under 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.

13 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 and CESG IA Policy Portfolio.

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

(a) provide the Authority within twenty (20) working days 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, the Security Policy Framework and CESG IA Policy Portfolio;

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

(e) ensure that any Personal Data that is no longer required is securely erased in accordance with HMG IA Standard No. 5.

**Networking**

15 The Authority requires that any Authority Data handled by the Supplier Solution and then transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted. The approach to encryption should make use of relevant open standards, and consider use of relevant products or system components which have been formally assured through a certification process such as Commercial Product Assurance (CPA) by CESG or an equivalent body approved by the Authority.

16 The Authority requires that the configuration, hardening 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.

17 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



This document is based on Schedule 2.4 of the Crown Commercial Services Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

boundaries of the UK. This shall be done in accordance with Security Policy Framework and CESG IA Policy Portfolio.

18 Any use of Cloud based services in connection with this agreement shall be required to implement CESG Cloud Security principles.

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

**Security Architectures**

20 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 Data.

21 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 and seek guidance from recognised security professionals with the appropriate skills such as those on the CESG Service Catalogue (https://www.ncsc.gov.uk/section/products-services/all-products-services-categories).

**Personnel Security**

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

23 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 CPNI 'Personnel Security Risk Assessment' available at: https://www.cpni.gov.uk/system/files/documents/46/06/Personnel-security-risk-assessment-a-guide-4th-edition.pdf

24 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.

25 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.



This document is based on Schedule 2.4 of the Crown Commercial Services Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

26 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.

27 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.

28 Where the Supplier or Sub-contractor 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 one (1) Working Day.

**Identity, Authentication and Access Control**

29 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 from local or remote devices. 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 for the Term.

30 The access control regime shall be compliant with ISO/IEC 27001 and ISO/IEC 27002, the Security Policy Framework, and the CESG IA Policy Portfolio.

**Audit and Monitoring**

31 The Supplier shall collect audit records (system logs) 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 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 mobile User Devices, desktops and server operating systems and security alerts from third party security software.

(c) compliance with ISO/IEC 27001 and ISO/IEC 27002, the Security Policy Framework, and the CESG IA Policy Portfolio.

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



This document is based on Schedule 2.4 of the Crown Commercial Services Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

33 The Supplier shall retain audit records collected in compliance with Paragraph 31 for the Term.

**Accreditation**

34 The Supplier shall deliver an accreditable Supplier System compliant with the policies and standards referred to in this Schedule which may change from time to time in accordance with Schedule 8.2 (Change Control Procedure).

35 The Supplier System shall be subject to Accreditation in accordance with this Schedule. Prior to the Supplier System becoming operational, the Supplier shall provide to the Authority, on request all of the information needed to construct a Risk Management and Accreditation Document Set (RMADS) in accordance with the provisions of this Schedule, for approval by the Accreditor.

36 The Supplier shall work with the Accreditor to ensure that the Supplier System achieves Accreditation within the timeframes specified in Schedule 6.1 (Implementation Plan).

37 Accreditation will be the responsibility of the Authority and carried out in accordance with Security Policy Framework and CESG IA Policy Portfolio undertaken by the Authority designated Accreditor:

(a) not less frequently than annually; and

(b) following any of the changes detailed within the RMADS.

38 The Supplier shall ensure that the Accreditor has approved any change to the Supplier System, including to the configuration or functionality of the Supplier System, before any such change is implemented and subsequently accredited.

39 Where changes to the Supplier System are required for whatever reason, the Supplier shall ensure that the changes are implemented in an appropriately secure manner, ensuring that no additional vulnerabilities are introduced into the system. The Supplier shall ensure that the Accreditor is informed about any changes at the earliest possible opportunity, using an agreed and approved method of communication between the Supplier and Accreditor or nominated representatives. If the Accreditor does not approve the change, the Supplier must rectify the changes at its cost, at the earliest possible opportunity.

40 Within 21 months after the Effective Date, the Supplier shall have a fully developed Risk Management and Accreditation Document Set (RMADS) in accordance with the Security Policy Framework and the Service Description that it will maintain throughout service delivery and make changes to, as and when they occur. The Supplier will comply with, and shall ensure that all Sub-contractors comply with and shall assist the Authority in complying with the RMADS, which shall:

(a) be owned by the Authority;

(b) comply with the Security Policy of the Supplier System (which covers the Supplier System, and includes any part of the Supplier System which is off-shored);



This document is based on Schedule 2.4 of the Crown Commercial Services Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

(c) be discussed and agreed with the Accreditor who shall specify the security policies, risks, measures and procedures with which the Supplier shall comply; and

(d) be kept up to date.

41 The Supplier shall ensure that all documents supporting any RMADS documentation are available for review, including cross-checking with the Supplier System, as required at any time by the Authority.

42 The Supplier shall, by use of a proactive security management regime, maintain the security Accreditation of the Supplier System including by:

(a) providing appropriate security controls including protecting applications, data, networks, systems and physical environment;

(b) responding to a changing threat, risk and vulnerability environment; and

(c) maintaining a level of security that is based upon the risks assessed within the RMADS.

43 The Supplier shall comply with the relevant RMADS and codes of connection in respect of all other systems and all business processes under the security control of the Authority or third parties that the Supplier has or requires access to in carrying out its obligations under this Agreement.

44 Any changes to the RMADS or the countermeasures contained therein which change the obligations on the Supplier shall be subject to the Change Control Procedure.

45 The Supplier shall comply with the agreed RMADS for the Authority Premises and Sites and shall ensure that its Sub-contractor providing related services for the Authority Premises and Sites also comply, where necessary, with the agreed RMADS provisions relating to the Authority Premises and Sites.

46 The Supplier shall develop, maintain and comply with security policies and procedures that are consistent with the Security Policy Framework and CESG IA Policy Portfolio.

47 The Supplier shall ensure that any communication links required for the provision of the Services are secured according to Security Policy Framework and CESG IA Policy Portfolio.

48 The Supplier shall ensure that Personal Data is protected at all times as agreed by the Authority designated SIRO and Accreditor and that the Personal Data is only to be retained for as long as it is required by the Authority.

**Business Continuity and Disaster Recovery**

49 The Supplier shall produce a Business Continuity Management System in accordance with BS ISO 22301, the Security Policy Framework and CESG IA Policy Portfolio.



This document is based on Schedule 2.4 of the Crown Commercial Services Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

## ANNEX 2: Security Management Plan

[…. ✂ ….]



This document is based on Schedule 2.4 of the Crown Commercial Services Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

This document is based on Schedule 2.4 of the Crown Commercial Services Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

This document is based on Schedule 2.4 of the Crown Commercial Services Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

This document is based on Schedule 2.4 of the Crown Commercial Services Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

This document is based on Schedule 2.4 of the Crown Commercial Services Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

This document is based on Schedule 2.4 of the Crown Commercial Services Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

This document is based on Schedule 2.4 of the Crown Commercial Services Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

This document is based on Schedule 2.4 of the Crown Commercial Services Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright

This document is based on Schedule 2.4 of the Crown Commercial Services Model Services Agreement v1.0 and has been adapted for use by the Emergency Services Mobile Communications Programme.

© Crown copyright