FUTURE SERVICE DELIVERY CONTRACT

SCHEDULE 2.4

SECURITY MANAGEMENT

CONTENTS

Clause	Heading	Page
1	INTRODUCTION	1
2	ACCREDITATION	2
3	ISMS	2
4	SECURITY MANAGEMENT PLAN	5
5	AMENDMENT AND REVISION OF THE ISMS AND SECURITY MANAGEMENT PLAN	6
6	SECURITY TESTING	7
7	ISMS COMPLIANCE	8
8	BREACH OF SECURITY	9
9	CO-OPERATION FOR BREACH OF SECURITY INVESTIGATIONS	10
10	VULNERABILITIES AND CORRECTIVE ACTION	11

APPENDIX 1: BASELINE SECURITY REQUIREMENTS 13

APPENDIX 2: SECURITY MANAGEMENT PLAN 64

APPENDIX 3: S&PDAL 65

SECURITY MANAGEMENT

1 INTRODUCTION

1.1 The Contractor acknowledges that the Authority places great emphasis on confidentiality, integrity and availability of information and consequently on the security of the Authority Premises and data (including Authority Data).

1.2 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.

1.3 The Contractor shall appoint a member of the Portfolio Management Board to be the Contractor Account Security Manager.

1.4 The Authority shall appoint a member of the Portfolio Management Board to be the Authority Security Officer.

1.5 The initial member of the Portfolio Management Board appointed by the Contractor for such purpose shall be the person named as such in Schedule 9.2 (Key Personnel) and the provisions of Clauses 17.3 to 17.7 (Key Personnel) shall apply in relation to such person.

1.6 The Contractor Account Security Manager shall be responsible, in consultation with the Authority Security Officer for:

(a) the implementation of all security arrangements concerning the Contractor Personnel, the area in which they are employed, their offices and their equipment; and

(b) the training and supervision of the Contractor Personnel; and shall ensure that the Contractor personnel; and procure that the Sub-Contractors comply with the security requirements set out in this Agreement.

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

1.8 The Contractor shall use as a minimum Good Industry Practice in the day to day operation of any system holding, transferring or processing Authority Data and any system that could directly or indirectly have an impact on that information, and shall ensure that Authority Data when being used or handled by the Contractor (or their agents or sub-contractors) in performing the Services remains under the effective control of the Contractor at all times.

1.9 The Contractor 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 within 5 Working Days to the Authority.

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

2 ACCREDITATION

2.1 The following Contractor solution elements shall all be accredited by the Accreditor prior to Operational Service Commencement Date:

(a) commercial grade encryption for remote management of data centre equipment / data;

(b) Assured LAN Interconnect (ALI) bandwidth / IP-Sec encryption for connectivity (FIPS 6.2) to Contractor premises; and

(c) remote protective monitoring from the Contractor's Security Operating Centre.

2.2 To support the achievement and ongoing maintenance of accreditation of the Contractor solution elements (as set out in Paragraph 2.1), the Contractor shall:

(d) within 90 Working Days from the Effective Date, deliver an accreditation plan (the format and contents of which are to be agreed with the Authority). Such accreditation plan is to provide details of how the Contractor can achieve and maintain accreditation of such Contractor solution elements and the relevant approvals and/or associated accreditations to be obtained and maintained; and

(e) prior to each Security Working Group (SWG) or as reasonably directed by the Authority, update the accreditation plan and present it to the accreditor and the Authority (SO1 Sy) at each Security Working Group (SWG); and

(f) ensure that such accreditation plan:

(i) satisfies the DAIS Accreditor that all systems will provide an overall level of protection commensurate with the BIA (detailed in the 'Security and Personal Data Aspects Letter') and risk appetite; and

(ii) reflects the current status of the IT Environment and accommodates all planned future Transformation, and is to be reviewed and updated once a month.

2.3 The Contractor acknowledges and agrees that it bears the risk of the Contractor solution elements identified in Paragraph 2.1 being accredited by the Accreditor and that the Contractor shall be responsible for all costs associated with any remedial work required in order to achieve such accreditation.

3 ISMS

3.1 By the date specified in the Transition Plan the Contractor shall develop and submit to the Authority for the Authority's approval in accordance with Paragraph 3.6 an ISMS (information security management system) for the purposes of this Agreement, which:

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

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

3.2 The Contractor acknowledges that the Authority places great emphasis on the reliability of the Services and confidentiality, integrity and availability of information and consequently on the

security 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 (to the extent falling under the control and responsibility of the Contractor) the Authority Premises, the Sites, the Contractor System, the Authority System and any IT, information and data (including the Authority Confidential Information and the Authority Data) to the extent used by the Authority or the Contractor in connection with this Agreement;

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

(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 contained in Appendix 1 (*Baseline Security Requirements*);

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

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

(vi) minimises the impact of any security incident relating to the Authority Premises and data (including Authority Data);

(vii) complies with:

(A) the security requirements as set out in this Schedule; and

(B) the security requirements as set out in Schedule 2.3 (Standards);

(viii) is in accordance with the Security Policy Framework provided that the consequences of any update to such Security Policy Framework including any additional costs are agreed by the Parties under the Change Control Procedure.

(ix) is appropriate to maintain the following at acceptable risk levels (defined by the Authority in the Security and Personal Data Aspects Letter (as amended from time to time in accordance with Paragraph 4.1 of Appendix 1) in respect of:

(A) loss of integrity of Authority Data;

(B) loss of confidentiality of Authority Data;

(C) unauthorised access to, use of, or interference with Authority Data by any person or organisation;

(D) unauthorised access to network elements (in respect of those elements of the network that are under the control of the Contractor), buildings, the Authority Premises and tools used by the Contractor in the provision of the Services;

(E) use of the applications or services within the control and responsibility of the Contractor by any third party in order to gain unauthorised access to any computer resource or Authority Data; and

(F) loss of availability of Authority Data due to any failure or compromise of the Services;

(d) documents the security incident management processes and incident response plans;

(e) document the vulnerability management policy including processes for identification of system vulnerabilities and assessment of the potential impact on the Services of any new threat, vulnerability or exploitation technique of which the Contractor becomes aware, prioritisation of security patches, testing of security patches, application of security patches, a process for Authority approvals of exceptions, and the reporting and audit mechanism detailing the efficacy of the patching policy; and

(f) be certified by (or by a person with the direct delegated authority of) a Contractor'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 25.11 (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 Contractor from time to time.

3.5 In the event that the Contractor becomes aware of any inconsistency in the provisions of the standards, guidance and policies set out in Paragraph 3.3, the Contractor shall immediately notify the Authority Representative of such inconsistency and the Authority Representative shall, as soon as practicable, notify the Contractor which provision the Contractor 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 Contractor immediately and thereafter operated and maintained in accordance with this Schedule. If the ISMS is not approved by the Authority, the Contractor shall amend it within 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 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 to the ISMS shall not relieve the Contractor of its obligations under this Schedule.

4 SECURITY MANAGEMENT PLAN

4.1 Within 60 Working Days after the Effective Date, the Contractor 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 initial Security Management Plan set out in Appendix 2;

(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 Contractor;

(d) detail the process for managing any security risks from Sub-contractors and third parties authorised by the Authority with access to the Services, and, to extent that the following are under the control of the Contractor (or their agents or sub-contractors), processes associated with the delivery of the Services, the Authority Premises, the Sites, the Contractor System, the Authority System 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, to extent that the following are under the control of the Contractor (or their agents or sub-contractors), and all processes associated with the delivery of the Services, including the Authority Premises, the Sites, the Contractor System, the Authority System and any IT, Information and data (including the Authority Confidential Information and the Authority Data) to the extent used by the Authority or the Contractor 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 Contractor 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 3.4);

(g) set out the plans for transiting all security arrangements and responsibilities from those in place at the Effective Date to those incorporated in the ISMS at the date set out in Schedule 6.1 (*Transition and Transformation Plans*) for the Contractor to meet the full obligations of the security requirements set out in this Schedule;

(h) set out the scope of the Authority System that is under the control of the Contractor;

(i) be structured in accordance with ISO/IEC 27001 and ISO/IEC 27002, cross-referencing if necessary to other Schedules which cover specific areas included within those standards;

(j) be written in plain English in language which is readily comprehensible to the staff of the Contractor 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

(k) be in accordance with 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 Contractor immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not approved by the Authority, the Contractor shall amend it within 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 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 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 Contractor 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 Contractor 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; and

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

5.2 Subject to paragraph 5.3 the Contractor shall provide the Authority with the results of such reviews as soon as reasonably practicable after their completion and amend the ISMS and Security Management Plan at no additional cost to the Authority. The results of the review shall include, without limitation:

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

(b) updates to the risk assessments;

(c) proposed modifications to respond to events that may impact on the ISMS including the security incident management process, incident response plans and general procedures and controls that affect information security; and

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

5.3 Subject to Paragraph 5.4, any change which the Contractor proposes to make to this Schedule 2.4 (Security Management), the ISMS or Security Management Plan (as a result of a review carried out pursuant to Paragraph 5.1, an Authority request, a 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 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 Contractor 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. Security Tests shall be designed and implemented by the Contractor so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Authority. Subject to compliance by the Contractor with the foregoing requirements, if any Security Tests adversely affect the Contractor’s ability to deliver the Services so as to meet the Target Performance Levels, the Contractor shall be granted relief against any resultant under-performance for the period of the Security Tests.

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

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

6.4 Where any Security Test carried out pursuant to Paragraphs 6.2 or 6.3 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Contractor shall promptly notify the Authority of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Contractor proposes to make in order to correct such failure or

weakness. Subject to the Authority's prior written approval, the Contractor shall implement such changes to the ISMS and the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Authority or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan is to address a non-compliance with the Baseline Security Requirements or security requirements as set out in the requirements of this Schedule, the change to the ISMS or Security Management Plan shall be at no cost to the Authority.

6.5 If any repeat Security Test carried out pursuant to Paragraph 6.4 reveals an actual or potential Breach of Security due to a Default or Defect of the Contractor exploiting the same root cause failure, such circumstance shall constitute a material Default for the purposes of Clause 32.1(b) (Rectification Plan Process).

7 ISMS COMPLIANCE

7.1 The Authority shall be entitled to carry out such security audits as it may reasonably deem necessary in order:

(a) to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001, the specific security requirements set out in this Schedule and the Baseline Security Requirements;

(b) to review and verify the integrity, confidentiality and security of any MOD Identifiable Information;

(c) to review the Contractor's and/or any Sub-contractor’s compliance with its obligations under this Schedule 2.4 (Security Compliance); and

(d) to review any Documentation Deliverable, including but not limited to any documents, reports and minutes which refer or relate to the Contractor Deliverables for the purposes of Paragraph 7.1.

7.2 The Authority shall use its reasonable endeavours to ensure that the conduct of each audit does not unreasonably disrupt the Contractor and/or Sub-contractor or delay the provision of the Contractor Deliverables and supplier information received by the Authority in connection with the audit shall be treated as confidential information.

7.3 The Contractor shall, and shall ensure that any Sub-contractor shall on demand provide the Authority and any relevant regulatory body, including the Contractor’s NSA/DSA, (and/or their agents or representatives), together “the Auditors”, with all reasonable co-operation and assistance in relation to each audit, including but not limited to:

(a) all information reasonably requested by the Authority within the permitted scope of the audit;

(b) reasonable access to any Sites controlled by the Contractor or any Associated Company and any Sub-contractor and to any equipment used (whether exclusively or non-exclusively) in the performance of the Agreement and, where such Sites and/or equipment are out of the control of the Contractor, shall secure sufficient rights of access for the Auditors as shall be necessary to allow audits to take place; and

(c) access to any relevant staff.

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 this Schedule and/or the Baseline Security Requirements is not being achieved by the Contractor, then the Authority shall notify the Contractor of the same and give the Contractor 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 Contractor 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 Contractor is found to be non-compliant with the principles and practices of ISO/IEC 27001, the specific security requirements set out in this Schedule and/or the Baseline Security Requirements then the Contractor 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.

7.6 The Authority shall endeavour to (but is not obliged to) provide at least 15 calendar days' notice of its intention to conduct an audit.

7.7 The Parties agree that they shall bear their own respective costs and expenses incurred in respect of compliance with their obligations under this Schedule, unless the audit identifies a material breach of the terms of this Paragraph 7 by the Contractor and/or Sub-contractor in which case the Contractor shall reimburse the Authority for all the Authority's reasonable costs incurred in the course of the audit.

8 BREACH OF SECURITY

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

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 Contractor 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 Contractor, if the mitigation adversely affects the Contractor’s ability to deliver the Services so as to meet the Target Performance Levels, the Contractor shall be granted relief against any resultant under-performance for

such period as the Authority, acting reasonably, may specify by written notice to the Contractor;

(iv) prevent a further Breach of Security 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**") on the Authority's request within 2 Working Days and without charge (where such requests are reasonably related to a possible incident or compromise); and

(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 this Schedule or the requirements of this Schedule, then any required change to the ISMS shall be at no cost to the Authority.

9 CO-OPERATION FOR BREACH OF SECURITY INVESTIGATIONS

9.1 Upon the occurrence of any Breach of Security:

(a) the Contractor shall procure that the Authority Representative and/or any other representative or adviser of the Authority shall have the right to enter any of the Sites or any property belonging to the Contractor or a Sub-Contractor and used in performing the Services in order to investigate such breach;

(b) the Contractor shall use its reasonable endeavours to make its employees (and those of Sub-Contractors) identified by the Authority Representative available to be interviewed by the Authority for the purposes of the investigation;

(c) the Contractor shall, subject to any legal restriction on their disclosure, provide all copies of documents, records or other material of any kind which may reasonably be required by the Authority for the purposes of the investigation. The Authority shall have the right to retain copies of any such material for use in connection with the investigation; and/or

(d) the Authority shall have the right to audit the Contractor's and/or Sub-Contractors' compliance with the Authority's security requirements set out in this Agreement, including this Schedule 2.4 and the Security Management Plan appended to it, in accordance with Schedule 7.5 *(Financial Reports and Audit Rights)*).

9.2 The Contractor shall, and shall procure that its Sub-Contractors shall, make available, and give reasonable assistance to the Authority Representative and/or any other representative or adviser of the Authority for the purposes of Paragraph 9.1.

9.3 Nothing in Paragraph 9.1 shall affect any entitlement to make Failure Charges and/or Withholding Deductions under this Agreement during the period in which the security investigation is subsisting or thereafter.

9.4 If the Authority's audit carried out pursuant to Paragraph 9.1(d) shows that the Contractor is not complying with the provisions of the Authority's security requirements set out in this Agreement including this Schedule 2.4 and the Security Management Plan appended to it, then the Contractor shall, at its own expense, rectify such non-compliance as soon as reasonably practicable.

10 VULNERABILITIES AND CORRECTIVE ACTION

10.1 The Authority and the Contractor 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.

10.2 The severity of threat vulnerabilities for Contractor COTS Software and Third Party COTS Software shall be categorised by the Contractor 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.

10.3 The Contractor 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 14 days of release, 'Important' within 30 days of release and all 'Other' within 60 Working Days of release, except where:

(a) the Contractor 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 Contractor asserts cannot be exploited within the context of a Service must be remedied by the Contractor 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 Contractor's ability to deliver the Services in which case the Contractor shall be granted an extension to such timescales of 5 days, provided the Contractor 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 Contractor under the processes defined in the ISMS.

10.4 The Contractor Solution and Transition and Transformation Plan shall include provisions for major version upgrades of all Contractor 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 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 Contractor 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.

10.5 The Contractor 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 Contractor) 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 Contractor) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS as developed under Paragraph 3.3(e) and through the processes described in Paragraph 17.12 of Appendix 1 (*Baseline Security Requirements)*;

(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 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 Contractor) 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 Contractor 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.

10.6 If the Contractor is unlikely to be able to mitigate the vulnerability within the timescales under Paragraph 10, the Contractor shall immediately notify the Authority.

10.7 A failure to comply with Paragraph 10.3 shall constitute a Notifiable Default, and the Contractor shall comply with the Rectification Plan Process.

APPENDIX 1: BASELINE SECURITY REQUIREMENTS

CONTENTS

Clause	Heading	Page
1	**HIGHER CLASSIFICATIONS**	14
2	**END USER DEVICES**	14
3	**DATA PROCESSING, STORAGE, MANAGEMENT AND DESTRUCTION**	14
4	**SECURITY & PERSONAL DATA ASPECTS LETTER (S&PDAL) (APPENDIX 3)**	15
5	**NETWORKING**	15
6	**SECURITY ARCHITECTURES**	15
7	**CYBER SECURITY**	15
8	**PERSONNEL SECURITY**	19
9	**IDENTITY, AUTHENTICATION AND ACCESS CONTROL**	20
10	**ADMISSION TO AUTHORITY PREMISES**	20
11	**DISCLOSURE OF PROTECTED INFORMATION**	21
12	**AUDIT AND MONITORING**	23
13	**USER ACCESS CONTROLS**	23
14	**RISK MANAGEMENT**	39
15	**BULK DATA MEASURES**	44
16	**CESG REQUIREMENTS AND RECOMMENDATIONS**	46
17	**NCSC CLOUD SECURITY PRINCIPLES**	48
18	**SANS CONTROLS**	54
19	**SECURITY AND INFORMATION GOVERNANCE**	63

1 HIGHER CLASSIFICATIONS

The Contractor 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 Contractor shall seek additional specific guidance from the Authority.

2 END USER DEVICES

2.1 When Authority data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or system component which has been formally assured through a recognised certification process of the UK Government Communications Electronics Security Group ("**CESG**") to at least Foundation Grade, for example, under the CESG Commercial Product Assurance scheme ("**CPA**").

2.2 Devices used to access or manage Authority data and services must be under the management authority of Authority or Contractor and have a minimum set of security policy configuration enforced. These devices must be placed into a 'known good' state prior to being provisioned into the management authority of the Authority. Unless otherwise agreed with the Authority in writing, all Contractor devices are expected to meet the set of security requirements set out in the CESG End User Devices Platform Security Guidance (https://www.gov.uk/government/collections/end-user-devices-security-guidance--2). Where the guidance highlights shortcomings in a particular platform the Contractor may wish to use, then these should be discussed with the Authority and a joint decision shall be taken on whether the residual risks are acceptable. Where the Contractor wishes to deviate from the CESG guidance, then this should be agreed in writing on a case by case basis with the Authority.

3 DATA PROCESSING, STORAGE, MANAGEMENT AND DESTRUCTION

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

3.2 The Contractor shall agree any change in location of data storage, processing and administration with the Authority in advance provided that no data shall be permitted to be stored or processed outside the UK.

3.3 The Contractor shall:

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

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

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

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

4 SECURITY & PERSONAL DATA ASPECTS LETTER (S&PDAL) (APPENDIX 3)

4.1 The Contractor hereby acknowledges the provisions set out in the S&PDAL. If the Authority amends the S&PDAL and, in the opinion of the Contractor, a change to the S&PDAL results in a material increase in the cost of providing the Services, the Contractor may submit a Change Request which shall be processed in accordance with the Change Control Procedure.

4.2 The Contractor shall protect all Information relating to the aspects designated OFFICIAL-SENSITIVE as identified in the S&PDAL in Appendix 3 to the Schedule 2.4, in accordance with the official security conditions contained in the Agreement or annexed to the S&PDAL.

4.3 The Contractor shall include the requirements and obligations set out in Paragraph 4.2 in any sub-contract placed in connection with or for the purposes of the Agreement which requires disclosure of OFFICIAL-SENSITIVE Information to the subcontractor or under which any Information relating to aspects designated as OFFICIAL-SENSITIVE is created by the subcontractor. The Contractor shall also include in the sub-contract a requirement for the subcontractor to flow the requirements of this Paragraph 4.3 to its subcontractors and through all levels of the supply chain to the lowest level where any OFFICIAL-SENSITIVE Information is handled.

5 NETWORKING

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

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

6 SECURITY ARCHITECTURES

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

6.2 When designing and configuring the IT Environment (to the extent that the IT Environment is within the control of the Contractor) the Contractor shall follow Good Industry Practice and seek guidance from the ISS Design Authority being the Authority's recognised security professionals with the appropriate skills for all bespoke or complex components of the Contractor Solution.

7 CYBER SECURITY

7.1 The Contractor acknowledges that the Authority has determined that the Security Risk Level for this Agreement is "high" (as defined in DEFSTAN 05-138) and that such Security Risk Level may be reassessed from time to time and notified by the Authority.

7.2 The Contractor shall, and shall procure that its Sub-Contractors shall:

(a) comply with DEFSTAN 05-138;

(b) complete the Cyber Security Model ("**CSM**") Risk Assessment Process in accordance with the Authority's instructions, ensuring that any change in the Security Risk Level is notified to any affected Sub-contractor, and complete a further CSM Risk Assessment or CSM Supplier Assurance Questionnaire where a change is proposed to the Contractor's supply chain which has or may have an impact on the Security Risk Level of this Agreement or on receipt of any reasonable request by the Authority;

(c) carry out the CSM Supplier Assurance Questionnaire no less than once in each year of this Agreement commencing on the first anniversary of completion of the CSM Supplier Assurance Questionnaire;

(d) having regard to the state of technological development, implement and maintain all appropriate technical and organisational security measures to discharge its obligations under this Paragraph 7 in accordance with Good Industry Practice and ISS and NCSC guidelines provided always that where there is a conflict between the Contractor's obligations under Paragraph 7.2(a) above and this Paragraph 7.2(d) the Contractor shall notify the Authority in accordance with the notification provisions in DEFSTAN 05-138 as soon as it becomes aware of the conflict and the Authority shall determine which standard or measure shall take precedence;

(e) comply with all Cyber Security Instructions notified to it by the Authority as soon as reasonably practicable;

(f) notify the JSyCC WARP in accordance with ISN 2014/02 as amended or updated from time to time and the Contractors NSA/DSA, and in the case of a Sub-contractor also notify the Contractor, immediately in writing as soon as they know or believe that a Breach of Security has or may have taken place providing full details of the circumstances of the incident and any mitigation measures already taken or intended to be taken;

(g) in coordination with its NSA/DSA, investigate any Breach of Security fully and promptly and co-operate with the Authority and its agents and representatives and its NSA/DSA to take all steps to mitigate the impact of the Breach of Security and minimise the likelihood of any further similar Breach of Security. For the avoidance of doubt, this shall include complying with any reasonable technical or organisational security measures deemed appropriate by the Contractors NSA/DSA in the circumstances and taking into account the Security Risk Level;

(h) consent to the Authority recording and using information obtained in relation to the Agreement for the purposes of the Cyber Security Model whether on the Supplier Cyber Protection Service or elsewhere. For the avoidance of doubt such information shall include the cyber security accreditation of the Contractor and / or Sub-contractor as appropriate; and

(i) include provisions equivalent to this Paragraph 7 in all Sub-contracts imposing provisions equivalent to this Paragraph 7 (the "**equivalent provisions**") and, where a Sub-Contractor breaches terms implementing this Paragraph in a Sub-contract, the Contractor

shall, and shall procure that its Sub-Contractors shall, in exercising their rights or remedies under the relevant Sub-contract:

(i) notify the Authority of any such breach and consult with the Authority regarding any remedial or other measures which are proposed as a consequence of such breach, taking the Authority's views into consideration; and

(ii) have regard to the equivalent provisions,

PROVIDED ALWAYS THAT where the Contractor has notified the Authority that it or one or more if its Sub-contractors cannot comply with Paragraphs 7.2(a) to 7.2(i) above the Authority and Contractor will seek to agree a Cyber Security Implementation Plan and where the Authority has agreed a Cyber Security Implementation Plan with the Contractor, the Contractor shall, and shall procure that its Sub-contractors shall, comply with such Cyber Security Implementation Plan until implementation is agreed to have been achieved whereupon Paragraphs 7.2(a) to 7.2(i) above shall apply in full. In the event that a Cyber Security Implementation Plan cannot be agreed the Dispute Resolution Procedure shall apply.

7.3 **Management Of Sub-Contractors**

(a) The Authority agrees that the Contractor shall be entitled to rely upon the self-certification by a Sub-contractor of its compliance with its obligations pursuant to Paragraph 7.2. In the event that a Sub-contractor is found to be in breach of its obligations in Paragraph 7.2, and where the Contractor has relied upon the Sub-contractor's self-certification, the Contractor shall not be held to be in breach of this paragraph.

(b) Where the Contractor becomes aware that a Sub-contractor is not complying with its obligations, the Contractor shall notify the Authority and provide full details of the Sub-contractor's non-compliance as soon as reasonably practicable and shall consult with the Authority as to the appropriate course of action which may include but not be limited to the agreement of a remedial plan or termination of the Sub-contract having regard to Paragraph 7.2(i).

(c) Having regard to the Authority's views, the Contractor shall take all reasonable measures to address any non-compliance of a Sub-contractor in accordance with the reasonable timescales required by the Authority. Where the Contractor fails to do so, this shall amount to a breach of this Paragraph 7.3 and the provisions of 7.2 or 7.3 as appropriate shall apply.

(d) The Contractor shall, and shall procure that its Sub-contractors shall, include provisions equivalent to this Paragraph 7.3 in all Sub-contracts which flow down the obligations set out in Paragraph 7.2.

7.4 **Records**

(a) The Contractor shall keep and maintain, and shall ensure that any Subcontractor shall keep and maintain, until 6 years after termination or expiry of this Agreement, or as long a period as may be agreed between the Parties, full and accurate records including but not limited to:

(i) details of all MOD Identifiable Information relating to the Contractor Deliverables provided under this Agreement; and

(ii) copies of all documents required to demonstrate compliance with DEFSTAN 05-138 and this Paragraph 7.4, including but not limited to any information used to inform the CSM Risk Assessment Process and to carry out the CSM Supplier Assurance Questionnaire, together with any certificates issued to the Contractor and/or Sub-contractor.

(b) The Contractor shall, and shall ensure that any Sub-contractor shall on request provide the Authority, the Authority's representatives and/or the Contractors NSA/DSA such access to those records as may be required in connection with this Agreement.

7.5 **Not Used**

7.6 **General**

(a) On termination or expiry of this Agreement the provisions of this Schedule 2.4 excepting 7.2 (b) and 7.2 (c) above shall continue in force so long as the Contractor and/or and Sub-contractor holds any MOD Identifiable Information relating to this Agreement.

(b) Termination or expiry of this Agreement shall not affect any rights, remedies, obligations or liabilities of the Parties under this Paragraph that have accrued up to the date of termination or expiry, including but not limited to the right to claim damages in respect of any breach of the Agreement which existed at or before the date of termination or expiry.

(c)

(i) The Contractor agrees that the Authority has absolute discretion to determine changes to DEFSTAN 05-138 and/or the Security Risk Level. In the event that there is such a change to DEFSTAN 05-138 or the Security Risk Level, then either Party may seek an adjustment to the Charges for any associated increase or decrease in costs and the Contractor may request an extension of time for compliance with such revised or amended DEFSTAN 05-138 or Security Risk Level provided always that the Contractor shall seek to mitigate the impact on time and cost to the extent which it is reasonably practicable to do so and further provided that such costs shall not be allowed unless they are considered to be appropriate, attributable to the Agreement and reasonable in all the circumstances.

(ii) Subject to 7.6(c)(i) above, where the Contractor seeks such adjustment or extension, the Authority will proceed in accordance with the Change Control Procedure or any agreed alternative change control procedure to determine the request for adjustment or extension. The Contractor must deliver a Contractor Change Proposal to the Authority within 8 weeks of the occurrence of the change in DEFSTAN 05-138 or Security Risk Level or such longer period as may be agreed by the Parties, identifying the impact of that change and accompanied by full details of the request for adjustment. For the avoidance of doubt, the Authority shall not be required to withdraw any Authority Notice of Change which may have been issued insofar as it relates to DEFSTAN 05-138 or the Security Risk Level whether or not the Contractor Change Proposal is rejected. In the event that the

Contractor does not agree with the Authority's determination, then the Dispute Resolution Procedure shall apply.

(d) The Contractor shall not recover any costs and/or other losses under or in connection with this Paragraph 7.6 where such costs and/or other losses are recoverable or have been recovered by the Contractor elsewhere in this Contract or otherwise. For the avoidance of doubt this shall include but not be limited to the cost of implementing any upgrades or changes to any information system or electronic communications network whether in response to a Breach of Security or otherwise, where the Contractor is able to or has recovered such sums in any other provision of this Agreement or has recovered such costs and/or losses in other contracts between the Contractor and the Authority or with other bodies.

8 PERSONNEL SECURITY

8.1 Contractor Personnel shall be subject to the Staff Vetting Procedures that include, as a minimum: employment history for at least the last three years, identity, unspent criminal convictions and right to work (including nationality and immigration status).

8.2 The Contractor shall provide comprehensive training for all Contractor Personnel and Authority Personnel (as applicable) in compliance with JSP 440 and the Authority's security requirements (as set out or referred to in this Agreement and the Security Management Plan). Such training shall be provided prior to the Contractor Personnel's engagement in the provision of any Service and thereafter on a regular basis throughout the Term as may be required due to changes in such requirements. The Contractor shall ensure that all Contractor Personnel are made aware of the relevant security arrangements and regulations on a continuous basis including through the appropriate display of security notices.

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

8.4 The Contractor shall prevent Contractor 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.

8.5 All Contractor 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.

8.6 Where the Contractor or Sub-Contractors grants increased IT privileges or access rights to Contractor Personnel, those Contractor 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 1 Working Day.

8.7 If and when directed by the Authority Representative, the Contractor shall provide the Authority with a signed statement from each and every Contractor Personnel that they understand that the Official Secrets Act 1911-1989 applies to them both during and after the Term and they shall adhere to its terms.

9 IDENTITY, AUTHENTICATION AND ACCESS CONTROL

The Contractor shall operate an access control regime to ensure all users and administrators of the Contractor Solution are uniquely identified and authenticated when accessing or administering the Services to the standards laid down in GPG 44 and GPG 45 (or their equivalent) at level 3 or above. Applying the 'principle of least privilege', users and administrators shall be allowed access only to those parts of the Contractor Solution they require. The Contractor shall retain an audit record of accesses.

10 ADMISSION TO AUTHORITY PREMISES

10.1 In respect of each Contractor Personnel, not less than ten (10) Working Days, unless by prior agreement, before such person is intended to first enter into or upon any Authority Premises in order to perform the Services, the Contractor shall provide the Authority Representative with details of such Contractor Person and any other details the Authority Representative may require (including full details of birthplace and parentage) together with details of the Authority Premises to which access is required and the capacity in which such person is concerned with the provision of the Services.

10.2 The Contractor Representative shall issue a photographic pass for all Contractor Personnel (pending approval from the Authority) who are security cleared to an appropriate level for the Authority Premises pursuant to Paragraph 10.1 on or before such person is intended to enter onto any Authority Premises in order to perform the Services. All such passes shall remain the property of the Authority and shall be surrendered on demand or on termination or expiry of this Agreement.

10.3 The Contractor shall ensure that the Contractor personnel and procure that the Sub-Contractors take such steps as may be necessary to obtain the security passes (including the taking of photographs, which the Contractor shall be able to provide to the Authority in electronic format).

10.4 A person not in possession of a pass who is required by the Contractor or any Sub-Contractor to attend the Authority Premises to provide emergency reactive services shall be allowed temporary admission to the Authority Premises provided that the Contractor shall, and where applicable shall ensure that any Sub-Contractor shall, procure that such individual is accompanied at all times whilst at or on the Authority Premises by a member of the Contractor or Sub-Contractor's staff who has been issued with a pass pursuant to Paragraph 10.2.

10.5 Whilst engaged at any Authority Premises the Contractor shall, and shall Procure that any Sub-Contractor shall, procure that all Contractor Personnel and other accompanied emergency reactive workers pursuant to Paragraph 10.3 comply with the Authority's policies relating to the conduct of staff and security arrangements as the Authority shall provide the Contractor from time to time.

10.6 Notwithstanding Paragraph 6.1, the Authority may refuse any person admission to any Authority Premises or require the removal of any person from any Authority Premises:

(a) if such person is not in possession of a pass pursuant to Paragraph 10.2 or is not an accompanied emergency reactive worker pursuant to Paragraph 10.3;

(b) if such person, in the Authority's reasonable opinion, represents a risk to themselves or property and the Authority Representative has given notice to the Contractor Representative to this effect;

(c) if the Authority has reasonable grounds for considering that the presence or conduct of such person at any Authority Premises is undesirable and the Authority Representative has given notice to the Contractor Representative to this effect;

(d) as part of a security investigation pursuant to Paragraph 9 and the Authority Representative has given notice to the Contractor Representative to this effect; and/or

(e) for any other security reason,

and the Authority's decision on any matter arising under this Paragraph shall be final and conclusive.

11 DISCLOSURE OF PROTECTED INFORMATION

11.1 In addition to its obligations pursuant to Clause 26 (Confidentiality), the Contractor shall not, either during or after the Term, do or permit to be done anything which it knows or ought reasonably to know may result in Protected Information being:

(a) without the prior consent in writing of the Authority Representative, disclosed to or acquired by a person who is a Non-UK National or who is a British subject by virtue only of a certificate of naturalisation in which his name was included;

(b) disclosed to or acquired by a person in respect of whom the Authority Representative has given to the Contractor Representative a notice, which had not been cancelled, stating that the Authority requires that Protected Information shall not be disclosed to that person;

(c) without the prior consent in writing of the Authority Representative, disclosed to or acquired by any person who is not a servant of the Contractor; or

(d) disclosed to or acquired by a person who is a servant of the Contractor except in a case where it is necessary for the proper performance of this Agreement that that person shall have the information.

Access to Protected Information

11.2 In addition to its obligations pursuant to Clause 26 (Confidentiality), the Contractor shall, both during and after the Term, take all reasonable steps to ensure:

(a) that no such person as is mentioned in Paragraph 11.2 shall have access to any thing or document under the control of the Contractor containing Protected Information except with the prior written consent of the Authority Representative;

(b) that no visitor to any premises in which there is anything to be supplied under this Agreement or where work in pursuance of this Agreement is being carried on shall see or discuss with the Contractor or any person employed by it any Protected Information unless the visitor is authorised in writing by the Authority Representative to do so;

(c) that no copies of anything supplied or to be supplied under this Agreement or of any portion of the work carried out in pursuance of this Agreement shall be taken by the Contractor except so far as may be necessary for the proper performance thereof or with the prior written consent of the Authority Representative, and that no such copy shall, without such consent, be published or otherwise circulated;

(d) that all Protected Information and every document, model, or other thing which contains or may reveal any such information is at all times strictly safeguarded, and that, except in so far as may be necessary for the proper performance of this Agreement or with the prior written consent of the Authority Representative, no copies of or extracts from any such document, model or thing shall be made or used and no designation or description which may reveal information about the nature or contents of any such document, model or thing shall be placed thereon; and

(e) that if the Authority Representative gives notice to the Contractor Representative at any time requiring the delivery to the Authority of any such document, model or thing that document, model or thing (including all copies thereof or extracts therefrom) shall forthwith be delivered to the Authority who shall be deemed to be the owner thereof and accordingly entitled to retain the same.

11.3 The decision of the Authority on the question of whether the Contractor has taken or is taking all reasonable steps as required by the provisions of Paragraph 11.2 shall be final and conclusive.

Contractor Personnel and Other Persons with Access to Protected Information

11.4 If and when directed by the Authority Representative, the Contractor Representative shall furnish full particulars of all Contractor Personnel and other persons who are at any time concerned with any Protected Information.

11.5 If at any time either during or after the Term it comes to the attention of the Contractor that any Contractor Personnel acting without lawful authority is seeking or has sought to obtain information concerning this Agreement or anything done or to be done in pursuance thereof, the matter shall be promptly reported by it to the Authority Representative and the report shall, in each case, be accompanied by a statement of the facts including, if possible, the name, address and occupation of that person. The Contractor shall be responsible for making all such arrangements as it may consider appropriate to ensure that if any such occurrence comes to the knowledge of any Contractor Personnel, that person shall promptly report the matter to the Contractor with a statement of the facts as referenced above.

11.6 The Contractor shall place every person employed by it or a Sub-Contractor who in his opinion has or shall have such knowledge of any Protected Information as to appreciate its significance, under a duty to the Contractor to observe the same obligations in relation to that matter as are imposed on the Contractor by paragraphs 11.1 and 11.2. The Contractor shall, if directed by the Authority Representative, place every person who is specified in the direction or is one of a class of persons so specified, under the like duty in relation to any Protected Information which may be specified in the direction or is one of a class of Protected Information so specified, and shall at all times use his best endeavours to ensure that every person upon whom obligations are imposed by virtue of Paragraph 11.2 observes the said obligations, and the Contractor shall give such instructions and information to every such person as may be necessary for that purpose, and shall, immediately upon becoming aware of any act or omission which is or would be a breach of the said obligations, report the facts to the Authority Representative with all necessary particulars.

12 AUDIT AND MONITORING

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

(a) Logs to facilitate the identification of the specific asset which makes every outbound request external to the IT Environment (to the extent that the IT Environment is within the control of the Contractor). To the extent the design of the Contractor 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 Contractor) and shall include: privileged account logon and logoff events, the start and termination of remote access sessions, security alerts from desktops and server operating systems and security alerts from third party security software.

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

12.3 The Contractor shall retain audit records collected in compliance with this Paragraph 10 for a period of at least 6 months.

13 USER ACCESS CONTROLS

13.1 Access Management

For all systems and users, the Contractor shall:

(a) maintain an accurate register of user profiles, such register to be aligned to Contractor Personnel and Authority Personnel (DBS Mil Pers and Vets) roles;

(b) ensure that the IT Environment is administered, managed, and controlled for Contractor Personnel and Authority Personnel (DBS Mil Pers and Vets);

(c) administer, approve, and grant access (within 1 hour following approval) to accounts of the IT Environment through the trusted and agreed route in accordance with vetting standards and role-based permissions with access granted on a 'need to know' basis;

(d) suspend access to accounts to the IT Environment is to be suspended within 1 hour following approval of suspension through the trusted and agreed route and delete accounts which have been continuously suspended for more than 3 months;

(e) provide verification report to the Authority (SO1 Sy) confirming the review of the register of user profiles has been conducted;

(f) verification and audit reports of all IT applications users to be provided on a quarterly basis to the Authority or as agreed; Content / format variable in agreement with SO1 Sy (for example, accounts suspended through failure to sign SyOps); and

(g) annually review and agree all forms and procedures produced in support of system access and change on request by the Authority (SO1 Sy).

13.2 **Password Management**

The Contractor shall manage and control passwords to IT Environment in accordance with 'CESG Information Standard 1 and 2, DBS SyOps, and DBS Mil Pers and Vets Security Policy Manual', including:

(a) ensure the IT Environment systems must force the End User to change the day one password once account access is granted; and

(b) ensure the IT Environment system must compel the End Users to use passwords which adhere to secure standards.

13.3 **User Account Authorisation**

The Contractor shall:

(a) manage the procedures for authorisation of new Contractor and DBS Mil Pers and Vets users and administer the password access systems relating to the IT Environment and action any Authority requests within 3 Working Days (or such timescales as agreed with the Authority);

(b) in respect of DEVNET, Microsoft Office desktop environments AgencyNet Production, JPA Applications Accounts TAS 001, 002 & 004, and other authority specified requested applications, require verification of authorisation and security clearance levels; and.

(c) in respect of SF applications, in addition to verification and security clearance levels, require a SF training certificate prior to despatch to the trusted and agreed route for approval.

13.4 **User Account Deletion**

The Contractor shall disable access to accounts to the IT Environment as follows:

(a) within 1 Working Day of a Contractor or the Authority (DBS Mil Pers and Vets) user ceasing to be authorised, or as notified by the Authority (Security Team), disable such user's authorisation (except where explicitly agreed with the Authority);

(b) disable access to any accounts not accessed for 1 continuous month;

(c) any disabled account not used within a further 3 month period, is to be then deleted except where explicitly agreed with the Authority (SO1 Sy); and

(d) provide a monthly report to the Authority (SO1 Sy) to identify the accounts which have been deleted in the previous month to which the report relates.

13.5 **Protective Monitoring solution**

The Contractor shall operate a GPG13 adherent 'Protective Monitoring' service providing a GPG18 adherent forensic capability and supported by robust incident response as follows:

(a) make available and monitor 'Protective Monitoring' solution across JPA and all associated applications at all times (except for any Service Downtime as agreed with the Authority);

(b) make available and monitor 'Protective Monitoring' solution across JPA and all associated applications at all times (except for any Service Downtime as agreed with the Authority);

(c) unless agreed with the Authority (SO1 Sy), all 'Protective Monitoring' software is to always be within one release of the current approved version (N-1) with a clear upgrade or migration path identified;

(d) all Patches and Updates are to be assessed for impact on system performance and tested before being applied in accordance with Patching requirements and timescales (contained in Appendix 3 (Patching Requirements and Timescales) to Annex M to Schedule 2.1) unless otherwise agreed with the Authority;

(e) the 'Protective Monitoring' solution must have a recovery point objective (RPO) of no more than 4 hours of logs lost due to DR/BC event and a recovery time objective (RTO) the same as the main JPA application (Oracle EBS);

(f) where 'Protective Monitoring' solution detects a Protective Monitoring SEV 1 or 2 event that the Contractor believes may be of interest to the Authority (SO1 Sy and/or MOD JCU), automatically notify the Authority (SO1 Sy and/or MOD JCU) within 1 hour of the observed event. Log files associated with the event are to be securely transmitted to the Joint Cyber Unit (JCU) for further analysis to maintain compliance with Op Augite;

(g) perform the 'Protective Monitoring' SOC service in accordance with Incident Resolution Matrix (Appendix 2 (Incident Resolution Matrix) of Annex M to Schedule 2.1);

(h) operate the Protective Monitoring Service in accordance with technical specifications. Remote administration to be carried out via the RLI and from MOD, HMG or List X sites;

(i) annually review logs which are on-boarded to the 'Protective Monitoring' system and, on request from the Authority, remove logs no longer required;

(j) produce and delivery to the Authority a monthly report to demonstrate the log collection is aligned with GPG13 requirements; and

(k) perform and, when requested by the Authority, provide evidence that the following are being performed:

    (i) ensure the service generates adequate audit events to support effective identification of suspicious activity;

    (ii) analysis such events in real time to identify potential compromises or inappropriate use of your service; and

(iii) where compromise or inappropriate use are confirmed, respond promptly in accordance with published response plan informing SO1 Security at the time or within 1 Working Day.

13.6 **Security Operation Centre**

The Contractor shall provide a Security Operation Centre (SOC) managed by an independent Contractor with continuous real time monitoring and real time auditing capability including fraud detection, for all MOD Systems and Applications managed by the Contractor. The service is to be in accordance with RMADS. The SOC shall perform as a minimum the following:

(a) investigate and report all anomalies to Authority (SO1 Sy) within 1 Working Days of detection;

(b) upon request from the Authority (SO1 Sy) provide specified audit reports;

(c) ensure dedicated DBS Mil Pers and Veterans monitoring and resultant logs/alerts are operated and managed by appropriately cleared, authorised and trained personnel;

(d) operate continuous monitoring / alerting supported by a robust 'Cyber Incident Response Plan' (in the form prescribed by the Authority from time to time); and

(e) be able to either implement or trigger an appropriate response to any identified incident in accordance with the 'Cyber Incident Response Policy'.

13.7 **Account Security Manager**

The Contractor shall appoint an Account Security Manager (ASM) to manage and co-ordinate account security activity with the Authority (SO1 Sy) which shall be a dedicated 'CESG' certified professional and is to be permanently based at Centurion (co-located with Authority Sy Staff) and ensure the account is appropriately managed and compliant with extant policies; the ASM will be the primary point of contact for all aspects of security.

13.8 **Information Asset Owner Support**

For all data that the Authority's Information Asset Owners (IAO) is responsible for, the Contractor shall manage such data to perform, as a minimum, the following:

(a) provide a point of contact with knowledge of the relevant information assets, who shall attend all meetings of the 'IAO Working Group';

(b) provide all requested input to quarterly returns as directed by the IAO; and

(c) provide all necessary support to the IAO (including the provision of requested data and Contractor personnel to work with the IAO) in completing Data Privacy Impact Assessments, Information Asset Registers and Data Flow Control Registers as the system Manager.

13.9 **Security Operating Procedures (SyOps)**

The Contractor shall:

(a) perform the requirements under the 'Security Operating Procedures (SyOps)' and all associated practices in accordance with the Standards and Authority policies as notified to the Contractor from time to time; and

(b) 3 months following the Effective Date and every year thereafter, review and update the 'Security Operating Procedures' and all associated practices. Any amendments are to be drafted using track changes (or equivalent) stating reasons for amendment. Provide and issue to the Authority (SO1 Sy) for approval prior to publication.

13.10 **Security Process and Procedure Documents**

The Contractor shall establish, implement, operate, monitor, maintain, review, and update (all reviews and updates to be on an enduring basis and to incorporate additional requirements as a result of changes in MOD policies or industry best practice and only following the authorisation of the Authority (SO1 SY)) the MP&V Security Process and Procedures documents (ISMS) in consultation with the Authority (SO1 Sy) and structured as per ISO 27001 requirements and to factor in any additional requirements detailed within MOD policies.

13.11 **Emerging Policy**

The Contractor shall:

(a) monitor and implement new HMG/MOD/DBS policy and processes as required by the Authority (SO1 Sy) and provide details and recommend the scope of any new DBS process and documents; and

(b) when any new security policy and/or process is issued by the Authority (SO1 Sy), identified by the Contractor (and notified to the Authority (SO1 Sy) within 5 Working Days), or otherwise notified to the Contractor by the Authority:

(i) provide a quarterly report of all new policies and/or processes issued to the Authority (SO1 Sy); and

(ii) produce an impact assessment and non-costed options for the implementation for each new Security policy and/or process within 20 Working Days of identification. Such options are to include two or more methods of implementation, noting the advantages and disadvantages of each, and subsequently recommending an option for implementation.

13.12 **Prior Authorisation**

Prior to any change to an existing system or the development of any new system (automated and manual), ensure that it has received written authorisation from the Defence Assurance & Information Security (DAIS) Accreditor (via the Authority (SO1 Sy) or their delegated representative) and ensure that all such changes comply with security policies by the following procedure:

(a) completing an 'Engineering Change Request' form to document any infrastructure changes in line with JSP604 Part 2 (Vols 1&2) for new system development and changes; and

(b) minor changes to systems to be requested in writing for approval by the DBS SAC/DAIS Accreditor.

13.13 **Compliance to Regulations**

The Contractor shall comply with Authority security regulations and abide by any MOD or 'Other Government Department' (OGD) regulations during visits to other sites.

13.14 **Disposal and Destruction**

The Contractor shall:

(a) dispose of all Authority material (equipment, media, documentation) in accordance with extant MOD security regulations;

(b) following such disposal, acquire and retain a disposal certificate for destruction when required under extant policy;

(c) all disposals and retention of destruction certification should be in accordance with extant regulations;

(d) material declared for disposal is to be stored and managed in accordance with security regulations pending destruction;

(e) all material to be accounted for at the point of disposal and or destruction in accordance with current regulations; and

(f) notify those who manage the asset / inventory list when an item is disposed of within 5 Working Days.

13.15 **Data Protection**

The Contractor shall:

(a) provide data privacy in accordance with Data Protection Legislation and the 'DBS Retention and Disposal Schedule';

(b) retain original and copy documents in accordance with 'Public Record Office' guidelines provided;

(c) support Information Commissioner's Office investigations and audit requests responding within given timescales;

(d) support the DBS 'Subject Access Requests' (SARs) team for responses to any Data Subject Access Requests for information in line with Data Protection Legislation;

(e) manage personal data records held on the IT Environment in accordance with Data Protection Legislation and the DBS Retention and Disposal Schedule;

(f) delete Personal Data records from the IT Environment upon request from the Authority IAO within 1 week of receipt of request;

(g) respond to Authority requests for assistance in response to audit/inspection requests by the ICO to demonstrate joint compliance with GDPR Article 28;

(h) ensure that it is complying with its obligations under GDPR Articles 32 to 36 (inclusive); and

(i) notify the Authority (DPO) immediately if it considers that any of the Authority's instructions infringe the Data Protection Legislation.

13.16 **Data Retention, Archiving and Disposal**

The Contractor shall:

(a) securely and efficiently, hold, archive, and dispose of Data (including reference data, metadata and associated documentation) in accordance with extant legislation and applicable Law and MOD and DBS policy;

(b) retain all Data in accordance with Data Protection Legislation, the 'DBS Retention Policy', and system specific documentation such as RMADS/DPIAs and, where the retention policy is deemed unclear, seek direction from the relevant Authority IAO;

(c) conduct the destruction of data in accordance with DBS and MOD Policy and NCSC Guidance;

(d) gain the prior written consent of the Authority (SO1 Sy) for the use of any third parties to conduct destruction of Authority Data. The Contractor acknowledge and agrees that the Authority will only consider CPNI-certified or List X companies;

(e) provide confirmation to the Authority (SO1 Sy) annually on every anniversary of the Effective Date that all soft and hard copy data held has been assessed and found to be in line with the DBS retention policy and relevant archiving and destruction activity has been undertaken;

(f) where there are gaps in capability to assess data within a system the Contractor must notify the Authority (SO1 Sy) in the form of a 'Risk And Issues Notice' (RAIN) for compliance and risk assessment requirements within 5 Working Days;

(g) apply Digital Continuity management in respect of information assets; and

(h) facilitate the transfer of information and data to MOD CIO archives.

13.17 **Risk Management Accreditation Documents Sets (RMADS)**

The Contractor shall develop and maintain 'Risk Management Accreditation Document Sets' (RMADS) for the IT Environment as follows:

(a) develop the RMADS for the IT Environment for approval by the SAC/DAIS Accreditor;

(b) on each anniversary of the Effective Date, conduct an annual review of IS1 / IS2 risk management components of the RMADS;

(c) update the RMADS as directed by the Authority (SO1 Sy);

(d) inform the Authority (SO1 Sy) when changes to the RMADS are required if the Authority is unaware;

(e) initiate update to the RMADS upon receipt of change to threat notification; and

(f) provide information to the Authority (SO1 Sy) on risk identification and management for all changes and new projects in a Security Aspects Document (SADs). SADs are to be reviewed when the associated system changes.

13.18 **Acceptance of Responsibility**

The Contractor shall:

(a) record and retain new starters signed acceptance of the 'Acceptable Use Policy' (AUP), SyOps, Data Protection Legislation, Official Secrets Act (OSA), the 'Breach Management, Confidentiality Agreement' and the 'New Starters Declarations' for all Contractor staff;

(b) ensure that signed acceptance is obtained prior to granting an End User authority to access any data or the IT Environment; and

(c) provide confirmation at the Authority (SWG) that the requirement is being met.

13.19 **IT Security Health Checks**

The Contractor shall:

(a) participate in DBS lead 'IT Security Health Checks' (ITSHCs) for the IT Environment (which shall not include MODNET, DWP DOI, or any applications hosted by these networks) which shall include test facilitation and the tracking, reporting, monitoring, remedial action through to completion;

(b) identify and manage risks with SAC/DAIS Accreditor;

(c) manage remediation through the development and maintenance of the 'Remediation Actions Register' (RAR);

(d) agree with the Authority (SO1 Sy) the ITSHC plan within 10 Working Days of the Effective Date and annually thereafter;

(e) provide output reports following ITSHCs within 10 Working Days of completion of ITSHC to Authority (SO1 Sy);

(f) remediate all risks identified during ITSHCs in coordination with SAC/DAIS Accreditor in accordance with the DBS Risk Management Framework;

(g) contribute to the DBS 'Master Remediation Actions Register' (MRAR) on request of the Authority;

(h) provide a managed service of 'Security Health Checks' (ITSHCs) of the IT Environment in accordance with the Authority's requirements;

(i) provide an annual penetration test for all contracted DBS infrastructure, systems and applications. This is to be done through an agreed rolling programme, produced by the Contractor and agreed by Authority (SO1 Sy);

(j) perform all required remediation within 3 months of issue of the penetration report unless otherwise agreed by Authority (SO1 Sy);

(k) advise the Authority (SO1 Sy) of any instance when the use of a system (manual or automated) is found to be in breach of the prescriptions of the systems accreditation within 1 Working Day; and

(l) ensure the ITSHC is conducted by an independent, NCSC approved Contractor utilising security cleared personnel conforming to nationality caveats, unless otherwise agreed by the Authority.

13.20 **Right of Access**

Within 2 working hours of request, the Contractor shall allow the Authority (SO1 Sy) unhindered access to test, inspect, analyse and audit the security functionality of the systems, and make audit trail data available to the Authority.

13.21 **Protective Security Audit**

The Contractor shall:

(a) develop an annual cycle of protective security audits in coordination with the Authority (SO1 Sy);

(b) manage and update on an annual basis the 'Protective Sy Audit Cycle' documentation and provide the Authority (SO1 Sy) with the updated annual audit report each October detailing the audit findings, areas of concern and mitigation measures for consideration;

(c) advise the Authority's (SO1 Sy) of any instance of Security concern or vulnerability within 1 Working Day of the occurrence; and

(d) present summary reporting of activity and findings at the 'Security Working Group' (SWG)

13.22 **Patch Management – Security Aspects**

The Contractor shall:

(a) monitor and report on Updates to Patches (where practicable) in accordance with the 'Patch Management Policy';

(b) report on any Updates (excluding any regular updates) to the Anti-Virus Software across all IT systems;

(c) apply all Patches (to be sourced from DOBUS in the first instance and, if not available, from the vendor's website) in accordance with the Patching requirements and timescales (Appendix 3 (Patching Requirements and Timescales) of Annex M to Schedule 2.1) subject to testing;

(d) monitor the deployment status for Patches and Updates to the Anti-Virus Software for all networked and non-networked CIS in accordance with Appendix 3 (Patching Requirements and Timescales) to Annex M to Schedule 2.1;

(e) support Sy Governance meetings (SWG and 'Assurance Strategy' meeting) by providing updates upon request detailing:

(i) Update status for AV deployed;

(ii) Patch deployment status; and

(iii) Patch history;

(f) review and manage all MODCERTS and report on the deployment of Patches to address the documented vulnerabilities identified to the Authority (SO1Sy); and

(g) notify the Authority (SO1 Sy) where Patches cannot be deployed within indicated timelines.

13.23 **Security Awareness and Oversight**

The Contractor shall:

(a) maintain Security awareness and oversight of Contractor supplied systems and infrastructure notifying the Authority of any perceived security weaknesses, potential or otherwise and request written temporary approval to operate a system until such time as the deficiency is corrected;

(b) notify the Authority in writing immediately upon discovery of a perceived security weakness; and

(c) report all Security breaches in accordance with timelines detailed within JSP 541.

13.24 **Minimising Effects of a Malicious Attack**

The Contractor shall:

(a) minimise cross-infection following discovery of a malicious attack;

(b) perform immediate action to be in accordance with the 'Cyber Incident Response Plan' and the Authority (SO1 Sy) to be informed at the earliest opportunity; and

(c) follow procedures agreed with the Authority (SO1 Sy) for reporting and handling malicious content to take all reasonable measures to and assist in the formulation of a recovery plan.

13.25 **CANNEL Alert State**

The Contractor shall:

(a) ensure the correct 'CANNEL' state (being the MOD CIS Alert State) is applied against IT Environment;

(b) initiate all measures of the CANNEL alert state upon notification of change;

(c) produce, by the Operational Service Commencement Date, and maintain a 'CANNEL Alert Change Response Plan' in the form as directed by the Authority (SO1 Sy). This is to be kept up to date and agreed with the Authority (SO1 Sy); and

(d) monitor the CANNEL alert state, any changes are to be proactively implemented in accordance with the measures notified by the Authority, with an appropriate escalating or de-escalating response. Changes are to be notified to the Authority (SO1 Sy) within 1 Working Day of any change to the CANNEL alert state.

13.26 **Privileged User Access Control**

The Contractor shall:

(a) capture and maintain a record of Privileged Users;

(b) obtain signatures from End User with Privileged Users prior to them accessing the IT Environment (and each year thereafter) to confirm their acceptance of the 'Privileged Users SyOps';

(c) provide to the Authority (SO1 Sy) a quarterly report within 10 Working Days of the end of the relevant quarter detailing the numbers of Privileged Users and confirming the access requirement; and

(d) carry out a quarterly audit of Privileged Users to confirm an ongoing access requirement.

13.27 **Secure Design**

The Contractor shall:

(a) design and maintain a security architecture that fully satisfies the DAIS Accreditor and fully supports confidentiality, integrity and availability in accordance with the Business Impact Assessment (BIA) and Data Protection Legislation.

(b) ensure all systems provide an overall level of protection commensurate with the BIA (detailed in the Security & Personal Data Aspects Letter (S&PDAL) and risk appetite.

13.28 **Public Key Infrastructure (PKI)/Defence Public Key Infrastructure**

The Contractor shall:

(a) Implement and manage a Public Key Infrastructure (PKI) that utilises Certification (CA) or Registration Authority (RA) certificates across all Infrastructure, applications and networks

managed under this agreement in accordance with the MOD requirements unless agreed by the Authority (SO1 Sy);

(b) deploy an operational PKI infrastructure for Quester Net (for example, not including the MODNET and DOI) within a time frame to be determined by the Authority, but no later than 3 years following Operational Service Commencement Date;

(c) implement and maintain a Public Key Infrastructure (PKI) that utilises a Certification (CA) or Registration Authority (RA) across all Infrastructure, applications and networks managed under this agreement in accordance with the MOD requirements unless agreed by the Authority (SO1 Sy);

(d) use assured products in the correct configuration where possible and ensure that assurance is maintained through life. Any deviations to assured products must be approved by the Authority (SO1 Sy);

(e) an upstream Certificate/Registration Authority (CA/RA) must be approved by the Authority (SO1 Sy);

(f) replace all existing 'Self Signed Certificates' used across the DBS estate (being digital certificates internally created and automatically authorised) with certificates issued by a Defence Public Key Infrastructure (DPKI) Certification service; and

(g) extend the use of certificates across the DBS estate in accordance with requirements JSP604 (Leaflet 3005) and JSP40 (Leaflet 12).

13.29 **Encryption**

The Contractor shall provide, deliver, maintain and upgrade encryption protection on all Authority systems and applications (insofar as technically possible).

13.30 **JCU Log File Transmission**

The Contractor shall:

(a) securely transmit log files to JCU during supported hours in accordance with the Non-Functional Requirements & Service Availability (Appendix 1 of Annex M to Schedule 2.1), except for any Service Downtime as agreed with the Authority (SO1 Sy);

(b) forward the log files to JCU in Common Event Format (CEF) on request; and

(c) perform Incident Resolution to be in accordance with the Incident Resolution Matrix (Appendix 2 of Annex M to Schedule 2.1).

13.31 **Vulnerability Scanning**

The Contractor shall:

(a) provide, deliver, maintain and support a vulnerability scanning solution for the IT Environment;

(b) conduct a vulnerability scan of the IT Environment once a week; and

(c) send raw data scan results via an encrypted tunnel once per week to JCU.

13.32 **Intrusion Detection and Prevention**

The Contractor shall maintain a SNORT-compliant intrusion detection and prevention system (IDS/IPS) solution to protect the IT Environment as follows:

(a) such IDS/IPS solution to be in accordance with 'Option 1' of the JCU 'Sensor Wrap' requirements document v1.1 (issued on 15 June 2016);

(b) fully administer rule and signature sets on the IDS/IPS solution, including applying signature updates as required by JCU and matching GovCERT SNORT signatures against traffic;

(c) enable the ability to provide 'Full Packet Capture' (FPC) files when required by JCU, including ensuring the unencrypted network traffic will be tapped via 'Switch' port mirroring via FPC;

(d) ensure that the Service Levels for the SNORT-compliant IDS are in accordance with the NFR Matrix (Appendix 1 of Annex M to Schedule 2.1);

(e) maintain the capability to forward IDS/IPS alerts in real time to JCU over an encrypted channel via Arcsight Enterprise Security Module (ESM);

(f) apply the following signatures:

(i) Government-certified SNORT signatures when made available;

(ii) Intelligent-based signatures to be applied as supplied and required by JCU; and

(iii) DPKI certificates to be used on the IT Environment;

(g) forward the log files to JCU in Common Event Format (CEF) on request;

(h) apply all Patches for the transmission of the log files in accordance with Patching requirements and timescales (Appendix 3 of Annex M to Schedule 2.1); and

(i) perform Incident Resolution to be in accordance with the Incident Resolution Matrix (Appendix 2 of Annex M to Schedule 2.1).

13.33 **Information Assurance Maturity Model (IAMM)**

The Contractor shall:

(a) ensure Information Assurance Maturity Model (IAMM) Levels 1, 2 and 3 are delivered and maintained at all services applicable under the contract;

(b) provide responses to Authority IAMM audit requests / returns within 5 Working Days;

(c) generate and maintain the IAMM compliance plan that is approved by the Authority (SO1 Sy); and

(d) conduct a gap analysis of IAMM levels 1, 2 and 3 within 6 months of Effective Date and annually thereafter and provide the results to the Authority within 5 Working Days of completion, including a plan to achieve compliance.

13.34 **Data Flow Control**

The Contractor shall:

(a) report all data exchanges managed by the Contractor to the Data Flow Control Register (DFCR) Manager. Proactively review data exchange methods to ensure secure and pragmatic practices are applied;

(b) support the Authority in its annual audit of the DFCR;

(c) inform the DFCR Manager of new or changes to existing data flows prior to transmission;

(d) coordinate with the Authority to ensure mandated data sharing agreements are in place prior to data sharing commencing;

(e) inform the DFCR manager when a data flow ceases within 5 Working Days;

(f) complete annual returns for the DFCR verification process as requested by the DFCR Manager within 2 weeks of the request from the DFCR Manager; and

(g) identify any irregularities with a data exchange and report to the Authority within 1 Working Day of discovery of the irregularity.

13.35 **Data Protection Impact Assessments**

The Contractor shall:

(a) provide all reasonable assistance to the Authority in the preparation of any Data Protection Impact Assessment (DPIA) (an assessment by the Authority of the impact of the envisaged processing on the protection of Personal Data) prior to commencing any processing;

(b) provide responses to the Authority's requests for DPIA assistance within 5 Working Days and such responses to include:

(i) a systematic description of the envisaged processing operations and the purpose of the processing;

(ii) an assessment of the necessity and proportionality of the processing operations in relation to the Services;

(iii) an assessment of the risks to the rights and freedoms of Data Subjects; and

(iv) detail the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

13.36 **Data Storage**

The Contractor shall:

(a) ensure that all information for which DBS MP&V is the custodian and held or processed by the Contractor is marked, stored, afforded protection and disposed of in accordance with current regulations and in accordance with the regulations on aggregation of bulk data; and

(b) conduct an annual protective security audit for all systems and locations and report to the Authority (SO1 Sy) in the SWG following completion of the audit.

13.37 **Remote Working**

The Contractor shall:

(a) ensure that all Contractor Personnel and personnel of any Sub-Contractor (and their sub-contractors) who are delivering services to the Authority from a non-MOD location (including at the Data Centres or home working) provide annual assurance that JSP 440 and other applicable standards are being fully adhered to in line with the 'Security Aspects Letter' provided by the Authority

(b) produce an 'Annual Security Assurance Report' on an annual basis to be delivered to the Authority (SO1 Sy) by the end of August during the relevant year. Such report to be in the format and with the content as required by the Authority (SO1 Sy) (as notified to the Contractor from time to time) and include, but not be limited to, a confirmation that the Contractor is compliant with the 'Classified Materials Assessment Tool' (CMAT).

13.38 **Key & Combination Control**

The Contractor shall:

(a) maintain all Contractor managed keys and combinations in accordance with current regulatory requirements;

(b) report to the Authority on an annual basis on all Contractor managed keys and combinations in accordance with the JSP 440. This report is to be provided to the Authority within 1 week of completion and routinely reported to the Authority (SO1 Sy) at the SWG; and

(c) all discrepancies are to be reported to the Authority (SO1 Sy) within 2 Working Days.

13.39 **Authorised Access Lists**

The Contractor shall:

(a) maintain access lists for Data Centres, 'Branch Offices' and Communications rooms to ensure only authorised personnel are permitted access;

(b) lists to be reviewed and re-verified monthly; and

(c) access lists to be updated immediately of notification of the user's authorisation being rescinded.

13.40 **Identity/Warrant Card Production – Security Aspects**

The Contractor shall:

(a) securely issue, deliver identity documents and maintain auditable accounting for all blank, yet to be issued, DMASC, MOD F90, and 'Warrant Cards' held awaiting issue within DBS;

(b) maintain auditable records of secure storage and issue of identity documents;

(c) all discrepancies identified in the audit are to be reported to the Authority (SO1 Sy) immediately;

(d) all discrepancies identified in the audit are to be duly investigated by the Contractor and a report is to be submitted to the Authority (SO1 Sy);

(e) conduct a quarterly muster of all blank cards and report the findings to the Authority (SO1 Sy) within 5 Working Days of the completion;

(f) account for all blank DMASC, MOD F90 and Warrant Cards held within DBS (e.g. the blanks held on account, prior to production) and those DMASC MOD F90 and post production Warrant Cards stored at DBS prior to issuing to the Units; and

(g) storage and accounting procedures to be agreed with the Authority (SO1 Sy).

13.41 **Physical Security**

The Contractor shall:

(a) provide and maintain a secure physical environment at all Contractor managed locations utilised for the delivery of DBS Services;

(b) provide access controls and physical security procedures at all locations utilised for the delivery of DBS Services;

(c) produce a programme of Annual Audits of the physical controls at Contractor managed sites. The audit report is to be delivered to the SO1 Sy within 1 week of completion; and

(d) all procedures and controls are to be agreed by the relevant Authority SME prior to implementation.

13.42 The Contractor shall:

(a) ensure authorised visitors are allowed access to Contractor managed buildings and maintain visitor access lists for all Contractor managed buildings; and

(b) reconcile any issued passes on a daily basis and to investigate and report any discrepancies within 1 Working Day to the Authority (SO1 Sy) at all times.

14 RISK MANAGEMENT

14.1 Risk Management Framework

The Contractor shall comply with and contribute to the 'DBS Risk Management Framework' as follows:

(a) from the Effective Date, establish and fully implement a security risk management framework in accordance with the 'DBS Risk Management Framework';

(b) demonstrate conformance with a recognised standard which includes controls which articulate how well a governance framework manages a particular service; and

(c) maintain a documented framework for security governance, with policies governing key aspects of information security relevant to the service. Documentation is to be reviewed and agreed with the Authority (SO1 Sy) annually and is to compliment DBS Policy.

14.2 Risk Identification and Recording

The Contractor shall:

(a) maintain risk registers for contracted systems and applications and SME input to the 'DBS Risk Management Process';

(b) upon confirmation of a potential risk identified by the Contractor, a 'Risk And Information Notice' (RAIN) is to be raised and submitted to Authority (SO1 Sy);

(c) provide a suitable subject matter expert for attendance on an as required basis at all 'Security Risk Balance Case' meetings; and

(d) compile appropriately detailed RBCs, RAINs and remediation plans for all potential risks identified. Documents produced are to identify all potential courses of action, together with their associated advantages and disadvantages.

14.3 Accounting for Information Bearing Assets

The Contractor shall:

(a) account for information bearing assets (including hardware and software applications) for DBS throughout their life;

(b) conduct an annual review (every January) of the procurement, storage, distribution and decommission process for Information bearing Assets reporting the findings to the Authority (SO1 Sy) within 10 Working Days of completion;

(c) produce and maintain an auditable 'Information Bearing Asset Register' detailing all Hardware with sufficient information to enable the Authority to identify and track the

Hardware (which shall include as a minimum the make, model, serial number, storage capacity (if applicable));

(d) monitor the distribution and use of all 'Removable Media' (RM) on a quarterly basis (Jan, Apr, Jul, Oct);

(e) provide an annual report detailing the distribution and use of all 'Removable Media' (RM) report to be delivered to Authority (SO1 Sy) in Oct each year;

(f) conduct annual inventory check of all laptops. Report to be delivered to Authority (SO1 Sy) by Jul each year; and

(g) provide a report to the Authority within 10 Working Days of completion of every census, or inventory check.

14.4 **Security Point of Contact**

The Contractor shall:

(a) provide a security point of contact to respond to DBS users and customers in regard to security related queries and requests for information; and

(b) respond within 2 Working Days, to the following:

(i) 'First Resolving Group' to check and respond to reports that are provided via the Centre for the Protection of the National Infrastructure (CPNI) website reports);

(ii) 'First Resolving Group' to check and respond to MOD CERTs); and

(iii) Security Incidents reported to the Help Desk or the Contractor's Security staff.

14.5 **Security Incident Reporting**

The Contractor shall:

(a) provide to the Authority details of all security events across all DBS sites via submission into the 'DBS Security Incident Log';

(b) report all security breaches, security near misses, security incidents and security weaknesses identified to the Authority (SO1 Sy) within 1 Working Day. Reporting format is to be in accordance with the JSP 541;

(c) update the 'DBS Security Incident Log' accordingly within 1 Working Day;

(d) information arising from the investigation of security occurrences and incidents shall be protected and handled on a need-to-know basis, and documentation of these matters given a suitable protective marking on a case by case basis; and

(e) investigation reports ('Initial', 'Interim', and 'Final') to be provided to the Authority for submission into the Incident Log within the following timescales (Initial: 1 Working Day of

notification of the occurrence / Interim: As agreed with the Authority (SO1 Sy), Final: within 5 Working Days of completion of the investigation).

14.6 **Security Incident Reporting**

The Contractor shall:

(a) proactively, or as directed by the Authority (SO1 Sy) investigate all security breaches, security incidents, security weaknesses, potential incidents, or other event/occurrence;

(b) investigations to be completed in a proactive and timely manner and reported within the timescales at Paragraph 14.11;

(c) Investigation reports and updates are to contain sufficient information for the completion of the 'MISIRS submission form'; and

(d) submit all reports to the Authority (Integrated Security Assurance Team and SO1 Sy).

14.7 **Security Incident Mitigation**

The Contractor shall:

(a) propose and implement actions agreed with the Authority (SO1 Sy) to mitigate the impact of any security incident with a view to preventing a reoccurrence; and

(b) in response to a notified security incident, review initial information reported and propose measures to mitigate the impact of or prevent further instances of the event in question with measures adopted to be agreed with the Authority (SO1 Sy).

14.8 **Security Vetting**

The Contractor shall:

(a) ensure all Sub-Contractors (and their sub-contractors) hold required security clearance as detailed within this Schedule;

(b) ensure compliance with the vetting requirements and facilitate the provision of all information required to support the vetting process (initial or through life). Such security vetting and development vetting requirements are detailed within 'Schedule 2.4/S&PDAL' (as reviewed and amended by the Authority (SO1 Sy) from time to time). Developmental vetting is required for all Privileged Users and those security positions as identified by the Authority;

(c) maintain a database of all vetting clearances for Sub-Contractors ensuring vetting renewal actions are always completed prior to expiry;

(d) carry out security briefs and debriefs in accordance with extant regulations;

(e) notify the Authority (SO1 Sy) of any Sub-Contractor not holding the required vetting status prior to any engagement or commencement of employment at any DBS site. Appropriate

RBC SREs to be submitted to Authority (SO1 Sy) no later than one week prior to commencing employment in all instances; and

(f) on a monthly basis produce a list, categorised by each DBS site, of those Sub-Contractor and third party personnel working at risk with the prior approval of the Authority (SO1 Sy) and provide a copy to the Authority (SO1 Sy).

14.9 **Suitability to Hold Security Clearance**

The Contractor shall:

(a) inform the Authority (SO1 Sy) of any information which becomes available to the Contractor which may suggest that any of the Contractor Personnel may no longer be suitable for such work, even though security clearance may have previously been granted. Within 1 Working Day of such discovery, the Contractor shall raise and submit 'Aftercare Incident Reports' (AIR) in accordance with JSP440 and inform the Authority (SO1 Sy);

(b) where a Security Incident gives rise to an AIR, then confirmation that the AIR has been sent is always to be provided within the final report; and

(c) list the number of AIRs submitted in Annual Security Assurance Report.

14.10 **Security Education & Awareness**

The Contractor shall:

(a) provide initial, annual and ad-hoc security education to ensure all Contractor Personnel engaged in the provision of Authority services are aware of their security responsibilities and have undergone adequate training in the use, care, protection and handling of Personal Data;

(b) obtain annual assurance from Sub-Contractors and third parties that their employees are aware of their security responsibilities, and that assurance must be made available to the authority;

(c) provide annual assurance that Sub-Contractors receiving and processing authority data are aware of their security responsibilities which as flowed down through a 'Security and Personal Data Aspects Letter';

(d) develop and maintain and deliver annual security and information assurance briefs and deliver annually to all DBS Contractor employees;

(e) develop and deliver themed security awareness campaigns (posters, entries in DBS publications, all user messages). No more than 12 awareness campaigns per annum; and

(f) ensure Contractor staff complete periodic mandatory training as identified by the Authority (SO1 Sy).

14.11 **Freedom to Investigate**

The Contractor shall:

(a) allow any investigative body authorised by the Authority (SO1 Sy) free access to Contractor sites, records, information and staff deemed relevant to the investigation of any security occurrence; and

(b) upon request from the Authority (SO1 Sy) grant the nominated investigative body authorised by the Authority (SO1 Sy) free access to Contractor sites, records, information and staff deemed relevant to the investigation of any security occurrence.

14.12 **SAC Secondment**

The Contractor shall second a dedicated resource to act as the Security Assurance Coordinator (SAC) working directly for the Authority (SO1 Sy) and in close coordination with the DAIS Accreditor to provide specialist technical advice in support of the accreditation of contracted systems and applications. SAC to hold in date CESG Certified Professional Senior Information Risk Advisor certification (CCP SIRA) at all times.

14.13 **Crypto Services**

The Contractor shall

(a) provide 'Crypto' services, including a 'Custodian' and 'Deputy Custodian', for DBS MP&V and HMS Sultan in accordance with JSP 490 and DBS MP&V Security Policy Manual. Such 'Custodian' and 'Deputy Custodian' to be suitably qualified in accordance with applicable regulations. For the avoidance of doubt, the joint arrangement with HMS Sultan is location-specific and is not applicable if the Services are no longer conducted from this location;

(b) support monthly audits and annual audits conducted by the Authority (Supervising Officer); and

(c) respond to 'National Crypto Authority Annual Audits'.

14.14 **Privileged Access Management**

The Contractor shall, in accordance with Paragraph 18.4, monitor and apply Privileged User access management controls as follows:

(a) all Privileged Users system usage to be recorded and analysed in accordance with Good Practice Guide (GPG) 13 at all times;

(b) monitoring information is to be retained for 7 years and made available within 5 Working Days of a formal request being submitted by the Authority (SO1 Sy);

(c) audit the accounts of Privileged Users to identify irregular activity and present a report to the Authority (SO1 Sy) at the 'Security Working Group' (SWG); and

(d) confirm any anomalies identified are to be reported to the Authority (SO1 Sy) within 1 Working Day and investigated immediately. An initial report is to be provided to the

Authority (SO1 Sy) within 1 Working Day followed up by regular briefs on a frequency agreed by the Authority (SO1 Sy).

15 BULK DATA MEASURES

15.1 The Contractor shall fully comply with the mandated NCSC Bulk Data Measures as published and periodically reviewed, in applying the requirements contained within this Schedule.

15.2 Understand and Actively Manage Vulnerabilities

The Contractor shall:

(a) using publicly available resources and available MOD resources (for example, the 'Cyber Security Information Sharing Partnership – CiSP' and the 'Ministry of Defence Computer Emergency Response Team – MODCERT'), maintain and actively manage an awareness of unmitigated vulnerabilities that are identified within DBS MP&V Information and Communications Technology assets, ensuring that awareness can be used to address risk and identify mitigations that are agreed with the authority in consideration for application;

(b) track, prioritise and mitigate in accordance with the regulations announced vulnerabilities for software packages, network equipment and operating systems in use in acceptable timescales agreed with the Authority (SO1 Sy);

(c) utilise 'CHECK'-certified third parties, as agreed with the Authority (SO1 Sy) for testing to confirm that internal expectations are matched by test findings;

(d) take all reasonable actions to ensure that known vulnerabilities in the Software and Hardware are mitigated;

(e) ensure all software on externally-accessible Hardware has had all security Patches applied (or vulnerabilities otherwise mitigated) in accordance with Appendix 3 of Annex M to Schedule 2.1 (Patching Requirements and Timescales);

(f) automate Patch management system across all systems and network attached devices;

(g) security test all Software and Applications for common vulnerabilities prior to handling live data;

(h) utilise market leading (both commercial sources and Open Source) external vulnerability intelligence services to maintain awareness of threats to the system;

(i) within tolerable levels of risk, carry out procedures in line with Good Industry Practice to identify vulnerable surfaces and investigate whether they can be removed or protected in a better fashion than would normally be dictated by an OFFICIAL system (including but not limited to implementing BPDM3). Where any vulnerability is identified within COTS software, vulnerabilities should be mitigated by other means until such time as a vendor patch or update is provided;

(j) provide an automated mechanism for vulnerability identification and management across the network as follows:

(i) prior to the scan taking place, advise the Authority on the technical and performance impact of conducting any full/partial scans and, working with the Authority and taking advice from JCU, ensure that the principles of such advice are incorporated into that scan and all future relevant scans; and

(ii) as any network-wide vulnerability scan is likely to have a performance impact (which could be exacerbated by the nature of the scan and the frequency at which they are conducted), undertake scans at a point which will minimise any disruption to the Service (unless agreed otherwise with the Authority); and

(iii) scans of network vulnerability are to be at the frequency agreed with the Authority to ensure that all Authority (DBS Mil Pers and Veterans);

(k) enable and conduct effective vulnerability / event correlation to aid attack identification and verification of logging activities which are to be subject to continual analysis; and

(l) ensure that all logs are available to the protective monitoring system 100% of the time. Make available all such logs to the protective monitoring system.

15.3 **Unsupported Software/Hardware**

The Contractor shall:

(a) ensure no unsupported software is present within the IT Environment and its underlying infrastructure;

(b) ensure that all operating systems, software packages and networking equipment for components which handle or secure access to data are in support by the vendor or community; and

(c) brief the Authority (SO1 Sy) through the Security Working Group (SWG), if a component upgrade falls outside N-1.

15.4 **Bulk Data Access/Export**

The Contractor shall:

(a) ensure that all exporters and users of bulk information are known by personal user identification, location and download pattern, and that any deviations from the known pattern are detectable and that an alert is raised where a deviation occurs;

(b) establish monitoring to detect unusual queries, attempted large scale exports of data or administrator access to data;

(c) from 3 months after the Effective Start, conduct quarterly tests of control measures in place and report failures to the Authority (SO1 Sy) together with mitigation measures to address the failure;

(d) for End Users whose permissions allow access to more than 1,000 records, their pattern of download over time is established within the 'Protective Monitoring System' as a behavioural characteristic; and

(e) with the download behaviour of End Users established, deviations from the pattern in excess of 10% (or such other percentage as notified by the Authority from time to time) of overall norm of download is reported to the Authority (SO1 Sy) within 1 Working Day of an event outside the known behaviour pattern being identified/confirmed.

15.5 **Rate Limiting**

The Contractor shall:

(a) rate-limited (managed, limited and controlled) End User access to bulk data is to agreed levels; and

(b) ensure that End Users are only permitted to download data in accordance with their established role-based permissions.

15.6 **Retain only Necessary Data**

The Contractor shall:

(a) ensure that all backups or copies of Authority data managed by the contract are held securely, and retained in accordance with the 'DBS Retention & Disposal Schedule';

(b) encrypt and store all copies of data required for temporary activities (including but not limited to error checking, Application code validation, error fixing, and all such other instances as agreed with the Authority) and delete immediately when no longer required or at the request of the Authority;

(c) ensure that no live data is used in test or development systems, unless these systems are protected to the same level as the production systems; and

(d) ensure that all uses of live data for testing purposes are approved by the Authority (SO1 Sy) prior to execution of the tests.

16 **CESG REQUIREMENTS AND RECOMMENDATIONS**

16.1 **Reduce Data Holdings**

Creation, Retention and Archiving (CRAD) has been conducted utilising an individual ‘whole record’ approach, with the record being retained for the longest retention period identified. In this regard it is considered that JPA and its associated applications are not wholly compliant with current Data protection Legislation and NCSC Requirements. Action is required in regard to the application of MOD data retention, archiving and destruction policy at the data item level whilst not detracting from the integrity of individual records within relational databases. The Contractor shall:

(a) ensure only active/necessary records are held within JPA and any supporting applications;

(b) identify scope for archiving within JPA and its associated applications and identify business processes impacted by archiving; and

(c) prior to archiving non-active data ensure mitigation measures are agreed with the Authority and in place.

16.2 **Intrusion Prevention Service**

The Contractor shall configure the 'Intrusion Prevention System' (IPS) to detect current threats and the currency against emerging threats to be maintained utilising threat intelligence signatures received from the Authority (MOD Certs) within 1 calendar day of receipt as follows:

(a) conduct testing on all industry security signatures (includes open source, commercial or any other viable source of security signatures) to ensure that the installation of such a signature will not trigger against a standard set of BAU traffic and, where it can be shown that a signature will trigger an interruption to BAU traffic, immediately notify the JCU;

(b) immediately following completion of testing in accordance with Paragraph 16.2(a), install such industry security signatures in the IPS;

(c) Oracle specific rules to be set in accordance with recommended guidance (including GPG13 and other sources at all time);

(d) F5 configuration to be always validated by pen-test during initial application installation; and

(e) employ 'White Listing' at all time.

16.3 **WEB Application Firewalls**

The Contractor shall:

(a) ensure that Web Application Firewall (WAF) protection is in place and active;

(b) ensure that Layer 7 Web Application Firewall protection is active at all times; and

(c) custom rules provided by, or configured with the aid of the Joint Cyber Unit or derived from commercial sources or internal intelligence are installed into the WAF after testing (if required).

16.4 **Bring Your Own Device (BYOD)**

The Contractor shall:

(a) where 'Bring Your Own Device' (BYOD) access is enabled with interactive functionality, follow guidance from Information Systems and Services (ISS) on deploying cross domain techniques to manage the risks;

(b) implement 'Cross Domain Measures' for BYOD in accordance with ISS requirements at all times; and

(c) ensure that all internet-facing BYOD is secured and delivered with user 2FA and dynamic identity confirmation compliant with the standards set out in GPG44 and GPG 45 at level 3 or above.

16.5 **Cryptography**

The Contractor shall:

(a) maintain the configuration of the cryptography used to protect system-system interactions at all times;

(b) where 'HMG Issued Cryptographic' systems or materials are used, then the requirements within JSP604, JSP490 and JSP491 are to be complied with;

(c) where commercial cryptographic products (hardware or software) are used, the Contractor is to maintain awareness of any vulnerabilities in the products used to ensure that cryptographic products remain suitable at all times; and

(d) where vulnerability has been identified in a commercial cryptographic product, the Contractor will do a risk analysis to identify what mitigations can be applied. All application of mitigations to be agreed with the Authority (SO1 Sy).

16.6 **Minimising Required Fields**

The Contractor shall actively reduce the impact of compromise by redacting, anonymising and limiting fields to the minimum required for each particular business use case.

16.7 **Network Management Infrastructure Separation**

The Contractor shall provide logically and physically separate network management infrastructure and terminals (with separate AD and supporting services) to reduce the risk of internet-borne attacks through Network access.

16.8 **Privileged Access Management & 2Factor Authentication**

The Contractor shall utilise 'Privileged Access Management' technologies, in conjunction with 'Two-Factor Authentication', to monitor and limit Privileged User actions on a ticket-by-ticket basis.

17 NCSC CLOUD SECURITY PRINCIPLES

17.1 **Data In Transit Protection**

The Contractor shall:

(a) ensure that End User data transiting networks is adequately protected against tampering and eavesdropping. The Contractor must always actively employ approved security measures to protect user data in transit;

(b) not use SSL versions or TLS versions earlier than 'Version 1.2';

(c) if it is unable to utilise a recommended security measure and no alternative is available, view such lack of security measure as a risk and treated as such;

(d) if an in-use 'Security Enforcing' function fails for any reason, advice is to be sought from the Authority (SO1 Sy) before any insecure transmission takes place;

(e) immediately notify the Authority if a transmission occurs which is subsequently found to be insecure in order that counter-compromise measures can be implemented;

(f) notify the Authority (SO1 Sy) prior to every transmission of live data where the Contractor is not able to utilise MOD recommended security measures; and

(g) ensure that 'Defence Public Key Infrastructure Services' are always utilised to provide Information Security.

17.2 **Asset Protection and Resilience – Identified Locations**

The Contractor shall ensure that all physical locations used to process, storing or manage user data are known to the Contractor and the Authority (SO1 Sy). Data is only to be processed and stored at locations identified and acceptable to the Authority (SO1 Sy).

17.3 **Asset Protection and Resilience – Security Standards**

The Contractor shall:

(a) ensure that the physical and emissions Security of all Data Centres meets the standards acceptable to the Authority at all times and provide a monthly report of such physical and emissions security to the Authority (SO1 Sy);

(b) ensure that Data Centres used are always certified to a recognised standard (which incorporates physical security). Such recognised standards include, but are not limited to, CSA CCM v3.0, SSAE-16 / ISAE 3402, and List X Standards;

(c) facilitate an annual inspection and audit of the security measures implemented within the Data Centres by an independent organisation (e.g. DAIS, or a body associated with the standard applied to the Data Centre) or the Authority (SO1 Sy, or personnel nominated by SO1 Sy), and will ensure that the results of the audit are available to the Authority (SO1 Sy) in accordance with a timetable to be agreed with the inspecting body prior to the inspection or audit occurring;

(d) ensure that 'TEMPEST' standards as identified in JSP440 are met at all times; and

(e) grant the Authority (SO1 Sy), or personnel nominated by the Authority (SO1 Sy), access to Data Centres within 5 Working Days of the request at all times.

17.4 **Asset Protection and Resilience – Data Security**

The Contractor shall:

(a) protection of 'Data at Rest' is to receive a level of protection commensurate with its protective marking and in consideration of impact if compromised;

(b) always employ encryption, obfuscation techniques or data storage 'sharding'; and

(c) at all times employ encryption to ensure that no data is written to disk in unencrypted form.

17.5 **Asset Protection and Resilience – Data Sanitation**

The Contractor shall apply 'Data Sanitisation' processes (utilising Authority or NCSC approved tools or devices) to ensure the secure destruction of data as follows:

(a) provide the capability to securely delete data at the field level in accordance with the data destruction standards of the Authority and National Cyber Security Centre (NCSC);

(b) ensure that any Storage media no longer required is sanitised according to a specified policy;

(c) provide evidence on request from the Authority that previously stored data cannot be accessed by others after storage media is released.

17.6 **Asset Protection and Resilience – Destruction and Disposal**

The Contractor shall:

(a) dispose of all hardware and other information bearing equipment in accordance with the 'CPNI Destruction Standard ' commensurate with the level of information carried on the asset;

(b) ensure a destruction service which specialises in secure disposal of equipment, which has been assessed against a recognised standard, is utilised; and

(c) coordinated equipment disposal with Asset owners and appropriate records maintained in accordance with asset management process.

17.7 **Asset Protection and Resilience – Resilience and Availability**

The Contractor shall:

(a) ensure 'Physical Resilience' and 'Availability' in accordance with the requirements contained in Schedule 8.6 (Business Continuity & Disaster Recovery) and ensure that such minimum levels of service availability are specified in any service level agreement with Sub-Contractors; and

(b) provide details and evidence to the Authority on request of how the Contractor has designed its solution to be resilient. The Contractor acknowledges that any support services in third party contracts not provided as a contractual obligation (for example, performed through 'reasonable endeavours') shall be deemed to have no guaranteed support for the purpose of this Paragraph 17.7.

17.8 **Separation between users**

When implementing a shared cloud service, the Contractor shall:

(a) ensure the separation between cloud tenants;

(b) provide evidenced assurance as to the integrity of separation of tenants within the cloud services prior to implementation of the shared cloud service and annually thereafter for the life of the service; and

(c) carry out penetration testing of the shared cloud service to ensure the products and security controls have been configured in accordance with Good Industry Practice and that there are no common or publicly known vulnerabilities in the tested components (at the time of the test) and ensure that such penetration testers are appropriately qualified (for example, individuals certified under the 'CHECK', CREST', or 'Tiger schemes).

17.9 **Governance and Compliance**

The Contractor shall:

(a) abide by the DBS MP&V Security Information Assurance Risk Governance process;

(b) security and information security are to be included as part of the Contractor's financial and operational risk reporting mechanisms, ensuring that the board would be kept informed of security and information risks;

(c) demonstrate conformance with a recognised standard which includes controls which articulate how well a governance framework manages a particular service at all times;

(d) nominate a clearly identified, and named, board representative (or a person with the direct delegated authority) who is responsible for the security of the cloud service. This is typically someone with the title ‘Chief Security Officer’, ‘Chief Information Officer’ or ‘Chief Technical Officer’. Changes to the nominated individual are to be notified to the Authority (SO1 Sy) within 5 Working Days of being made;

(e) maintain a documented framework for security governance, with policies governing key aspects of information security relevant to the service. Documentation is to be reviewed and agreed with the Authority (SO1 Sy) annually; and

(f) identify and ensure compliance with applicable legal and regulatory requirements. Non-compliance should be notified to the Authority (SO1 Sy) within 5 Working Days of discovery, together with details of mitigation measures adopted.

17.10 **Configuration and Change Management**

The Contractor shall:

(a) ensure that Configuration and Change Management Procedures are implemented such that all network assets are accountable, and their configuration status is known;

(b) the status, location and configuration of service components (both hardware and software) are to be continuously tracked throughout their lifetime; and

(c) assess all Changes for potential security impact, then managed and tracked through to completion. The Service Contractor provides evidence of this to the Authority (SO1 Sy) through the Security led 'Assurance Strategy' meeting.

17.11 **Operational Security - Vulnerability Management**

The Contractor shall:

(a) deploy a network wide capability to identify vulnerabilities which have been determined and listed by known reliable (commercial and Open Source) vulnerability intelligence sources;

(b) at a frequency to be agreed with the Authority (SO1 Sy), provide evidence that the following are being undertaken:

(i) potential new threats, vulnerabilities or exploitation techniques which could affect service delivery are assessed and corrective action is taken as required; and

(ii) relevant sources of information relating to threat, vulnerability and exploitation techniques are monitored and the severity of threats and vulnerabilities is considered within the context of the business and this information is used to prioritise the implementation of mitigations;

(c) track known vulnerabilities using a suitable risk management process until mitigations have been deployed and tested and demonstrate assurance conformance with a recognised standard. Any non-conformance of this Paragraph is to be notified to the Authority (SO1 Sy) within 5 Working Days; and

(d) provide timescales for implementing mitigations for the Authority's approval.

17.12 **Operational Security - Protective Monitoring.**

The Contractor shall:

(a) operate a GPG13 adherent Protective Monitoring service providing a GPG18 adherent forensic capability and supported by robust incident response;

(b) perform the Protective Monitoring service should be in accordance with Incident Resolution Matrix (Appendix 2 of Annex M to Schedule 2.1);

(c) when requested by the Authority, provide evidence that the following are being met:

(i) the service generates adequate audit events to support effective identification of suspicious activity;

(ii) these events are analysed in real time (24/7) to identify potential compromises or inappropriate use of your service; and

(iii) where compromise or inappropriate use are confirmed the Contractor is to respond promptly in accordance with published response plan informing SO1 Security at the time or within 1 Working Day; and

(d) demonstrate conformance with a recognised standard and any non-conformance is to be notified to the Authority (SO1 Sy) within 5 Working Days of discovery.

17.13 **Operational Security: Incident Management**

The Contractor shall:

(a) comply with the measures defined in the DBS Cyber Response Plan, and the DBS Incident Response Plan;

(b) processes and procedures to manage security incidents are to be in place 100% of the time;

(c) security incidents are to be reported in acceptable timescales and formats as detailed within the DBS Cyber Incident Response Plan. The Authority (SO1 Sy) is to be informed at the earliest opportunity, and within 1 Working Day; and

(d) demonstrate conformance with a recognised standard and any non-conformance is to be notified to the Authority (SO1 Sy) within 5 Working Days of discovery.

17.14 **Personnel Security**

The Contractor shall:

(a) conduct personnel security activities (including personnel screening) to ensure that only those personnel who have a need to access the systems and data are able to do so including, but not limited to:

(i) thorough enquiries into identity, nationality (including right to remain and work in the UK), previous employment record and a criminal records check covering both spent and unspent convictions; unspent convictions only are considered as part of the recruitment process through the Baseline Personnel Security Standard;

(ii) National Security Vetting to an appropriate level dependent on the individual requirement of the role;

(iii) supervision of personnel, including for Developed Vetting (DV) holders, an annual Security Appraisal of an individual's continuing suitability for clearance;

(iv) processes for reporting changes in personal circumstance, and issues/incidents that could give rise to concerns as to an individual's loyalty, reliability or integrity; and

(v) enhanced supervision or limited access to information, for individuals whose loyalty, reliability or trustworthiness is a concern and potentially a risk to sensitive assets or classified information; and

(b) conduct personnel screening with the level of screening required dictated by access levels as agreed with the Authority (SO1 Sy) and the DBS Vetting Policy and require any Sub-Contractor to conduct the same screening requirements.

17.15 **Secure Development.**

The Contractor shall:

(a) ensure that services are designed and developed to identify and mitigate threats to their security. Security is to be considered as an important factor in all elements of system development;

(b) provide evidence of the controls in place to ensure the security of the Service in response to a request from the Authority (SO1 Sy) within a timescale to be agreed;

(c) ensure that system development adheres to a secure development standard or recognised good practice at all times;

(d) review all new and evolving threats in the context of impact upon the Service;

(e) carry out all development in line with industry good practice regarding secure design, coding, testing and deployment; and

(f) ensure that 'Configuration Management' processes are in place to ensure the integrity of the solution through development, testing and deployment at all times.

17.16 **Supply Chain Security**

The Contractor shall:

(a) ensure its supply chain satisfactorily meets all of the security principles required of Sub-Contractors in this Agreement and demonstrate to the Authority on request that the security controls which are applicable to the system are enforced through their supply chain;

(b) maintain an asset database that contains configuration information against each assets, with the capability to identify the addition and removal of assets, and automatically record the configuration of a newly added asset, and alert the asset owner upon removal of a current asset;

(c) have a comprehensive inventory of assets connected to the network;

(d) manage the configuration of all connected devices by remote means;

(e) ensure that records of each 'Dynamic Host Configuration Protocol' allocation and release are maintained for a period of 6 months; and

(f) demonstrate supply chain security conformance with a recognised standard and any non-conformance is to be notified to the Authority (SO1 Sy) within 5 Working Days of discovery.

18 **SANS CONTROLS**

18.1 **SANS Control 1 – Inventory of Authorised and Unauthorised Devices**

The Contractor shall, using the Information Bearing Asset Register, actively manage (inventory, track and correct) all Hardware used within the IT Environment so that only authorised devices are given access and authorised, and unmanaged devices are found and prevented from gaining access.

18.2 **SANS Control 2 – Inventory of Authorised and Unauthorised Software**

The Contractor shall:

(a) implement a service for managing software assets for the identifying network users and managing licensing, versioning and the prevention of the execution of unauthorised software;

(b) maintain an automated database of all software assets (including all instances of Active Directory), to include version, patch, licence, patch and accreditation status. Applicable across all environments and operating systems;

(c) implement a white listing system, whereby only known and approved software of a known configuration, patch and build are allowed to execute; and

(d) run Software in a manner whereby it does not pose a threat to other applications.

18.3 **SANS Control 3 – Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers**

The Contractor shall ensure that the management of configuration and Releases are secure which shall include, but not be limited to:

(a) standardised versions of applications where multiple instances are required with only required services running are to be deployed;

(b) the integrity of all applications and data files are to be established;

(c) where available, deploying secure methods of communication and connection between network management protocols;

(d) monitoring the configuration of all Software;

(e) maintaining Software Port Control, Allocation and usage are to be monitored; and

(f) managing and deploying 'System Configuration Policies' and other associated objects.

18.4 **SANS Control 5 – Controlled Use of Administrative Privileges**

The Contractor shall control the use of Administrative privileges for access to the IT Environment by performing the following:

(a) ensuring that the actions of Privileged Users are managed and are traceable through protective monitoring. Ensure that the principle of least privilege is applied;

(b) having knowledge of all accounts and applying particular measures to privileged account holders operating inside the boundary (such as 'Database Administrators');

(c) implement Two-Factor Authentication for DBS civil servant and Contractor Privileged Users;

(d) subject all privileged accounts to automated inventory collation;

(e) change all default passwords;

(f) all privileged account management functions (creation, privilege allocation, promotion, demotion, suspension and deletion) are to be captured for protective monitoring;

(g) permit all Privileged User account transactions on a ticket-by ticket basis; and

(h) implement the security requirements contained in this Schedule within the cloud environment.

18.5 **SANS Control 6 – Maintenance, Monitoring and Analysis of Audit Logs**

The Contractor shall provide maintenance, monitoring, and analysis of audit logs by performing the following:

(a) support the capability of the 'Protective Monitoring System' including analysis of logs captured;

(b) ensure that the 'Protective Monitoring System' always has access to at least two synchronised time sources;

(c) validate the audit logs for all connected Hardware and Software devices and processes to ensure that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction;

(d) where an application is capable of generating security audit logs, that capability such that is compliant with the protective monitoring requirement is to be activated to allow auditable activities to be recorded and made available to the 'Protective Monitoring System';

(e) ensure that the IT Environment systems record logs in a standardized format such as syslog entries or those outlined by the 'Common Event Expression' initiative;

(f) if systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format;

(g) ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed;

(h) actively review any reports identifying anomalies in logs at the intervals to be agreed with the Authority (SO1 Sy); and

(i) identify and bring to the attention of the Authority (SO1 Sy) any anomalous action, or action identified as being of a serious security nature, as soon as practicable.

18.6 **SANS Control 7 – Email and Web Browser Protection**

The Contractor shall:

(a) use only supported web browser and email clients; and

(b) ensure that all software (including browser and email clients) is in-support, licensed and, where practical, accredited (e.g. the use of a 'Commercial Off The Shelf' product may be accredited rather than the product itself).

18.7 **SANS Control 9 - Limitation and Control of Network Ports, Protocols, and Services**

The Contractor shall provide limitation and control of network ports by doing the following:

(a) manage all network ports within their area of responsibility;

(b) deactivating all Network 'Terminal Access Ports' (TAPs) unless required for use;

(c) monitor all Network TAPs for use and ensure that active ports are associated with a device;

(d) any change in status of a network port is to be captured by protective monitoring;

(e) removal or addition of an authorised device from a Network TAPs is to be alerted;

(f) prevent any connection to a network port of a device that has not previously been authorised; and

(g) whilst the network boundary will have protection, individual devices within the boundary are also to be protected within the capabilities of any operating system used.

18.8 **SANS Control 10 – Data Recovery Capability**

The Contractor shall provide data recovery capability by continuing to apply the principles of backing up, restoration of data, and testing for capability to restore which are applied during Transition into Transformation.

18.9 **SANS Control 11 – Secure Configurations for Network Devices**

The Contractor shall provide secure configurations for Network devices by doing the following:

(a) implement secure configuration of the network devices in accordance with JSP440 and JSP604, taking guidance from ISS;

(b) ensure it has the capability to compare firewall, router, and switch configuration against standard secure configurations defined for each type of network device in use in the organisation;

(c) document the security configuration of firewalls, routers, and switches to facilitate Authority and Configuration Control board review;

(d) ensure that any deviations from the standard configuration or updates to the standard configuration are documented and approved in a change control system;

(e) all new configuration rules beyond a baseline-hardened configuration that allow traffic to flow through network security devices, such as firewalls and network-based IPS, will be documented and recorded in a configuration management system, with a specific business reason for each change, a specific individual's name responsible for that business need, and an expected duration of the need;

(f) use automated tools to verify standard device configurations and detect changes. All alterations to such files will be logged and automatically reported to security personnel;

(g) manage network devices using two-factor authentication and encrypted sessions;

(h) install the latest stable version of any security-related updates on all network devices after appropriate testing has taken place to ensure non-interference with delivery;

(i) ensure that all Network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access, such machine being:

(i) isolated from the primary network;

(ii) not connected to the internet; and

(iii) not used for reading e-mail, composing documents, or surfing the Internet; and

(j) manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

18.10 **SANS Control 12 – Boundary Defence**

The Contractor shall implement effective boundary defence by performing the following:

(a) implement and maintain an effective boundary defence in accordance with JSP440 and JSP604, will take advice on boundary protection from ISS. The security measures implemented for the network shall include the capability to deny communications with (or limit data flow to) known malicious IP addresses (black lists), or limit access only to trusted sites (whitelists);

(b) carry out periodic Tests by sending packets from logon source IP addresses (non-routable or otherwise unused IP addresses) into the network to verify that they are not transmitted through network perimeters. Testing should take place at least once between each SWG;

(c) configure DMZ networks with monitoring systems (which may be built in to the IDS sensors or deployed as a separate technology) to record at least packet header information, and preferably full packet header and payloads of the traffic destined for or passing through the network border. This traffic should be sent to a properly configured Security Information Event Management (SIEM) or log analytics system so that events can be correlated from all devices on the network;

(d) network-based IDS sensors shall be deployed on Internet and extranet DMZ systems and networks which will look for unusual attack mechanisms and detect compromise of these systems;

(e) network-based IPS devices shall be deployed to complement IDS by blocking known bad signatures or the behaviour of potential attacks;

(f) require all DBS privileged user login access (including VPN, dial-up, and other forms of access that allow login to internal systems) to use two-factor authentication;

(g) all enterprise devices remotely logging into the internal network shall be managed by the enterprise, with remote control of their configuration, installed software, and patch levels. For third-party devices (for example, those belonging to Sub-Contractors), publish minimum security standards for access to the enterprise network and perform a security scan before allowing access;

(h) periodically scan for back-channel connections to the Internet that bypass the De-Militarised Zone (DMZ), including unauthorized Virtual Private Network (VPN) connections and dual-homed hosts connected to the enterprise network and to other networks via wireless, dial-up modems, or other mechanisms;

(i) deploy 'NetFlow' collection and analysis to DMZ network flows to detect anomalous activity;

(j) endeavour to identify covert channels exfiltrating data through the firewalls; and

(k) configure the built-in firewall session tracking mechanisms included in many commercial firewalls to identify Transmission Control Protocol (TCP) sessions that last an unusually long time for the given organization and firewall device, alerting personnel about the source and destination addresses associated with these long sessions.

18.11 **SANS Control 13 – Data Protection**

The Contractor shall:

(a) implement measures to comply with all data protection provisions as detailed in this Agreement and apply all SANS Security Control 13 data protection measures;

(b) ensure that those measures are carried through in to transformation, and ensure that increased capability of transformation is reflected in the manner in which the data protection measures are implemented;

(c) perform an assessment of data to identify sensitive information that requires the application of encryption and integrity controls;

(d) deploy an automated tool on the network perimeter that monitors for sensitive information (e.g., personally identifiable information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting information security personnel;

(e) conduct periodic scans of servers using automated tools to determine whether sensitive data (e.g., personally identifiable information, health, credit card, or classified information) is present on the system in clear text;

(f) configure systems so that they will not write data to USB tokens or USB hard drives and maintain an inventory of all authorized devices must be maintained;

(g) use network-based DLP solutions to monitor and control the flow of data within the network;

(h) report any anomalies that exceed the normal traffic patterns (as specified by the Authority);

(i) any anomalous activity is to be investigated in accordance with the incident management process;

(j) monitor all traffic leaving the organization and detect any unauthorized use of encryption;

(k) block access to known file transfer and e-mail exfiltration websites; and

(l) deploy host-based data loss prevention (DLP) to enforce Access Control Lists (ACLs) even when data is copied off a server.

18.12 **SANS Control 14 – Controlled Access**

The Contractor shall implement controlled access based on role and the principle of 'Need to Know' by performing the following:

(a) apply the access control methods and measures through SANS Security Control 14 and ensure that those measures are maintained throughout the Term, and ensure that any increased capability through Transformation is reflected in the manner in which the data protection measures are implemented;

(b) segment the network based on the label or classification level of the information stored on the servers;

(c) locate all sensitive information on separated Virtual Local Area Networks (VLANS) with firewall filtering to ensure that only authorized individuals are only able to communicate with systems necessary to fulfil their specific responsibilities;

(d) ensure that all communication of sensitive information over less-trusted networks is encrypted;

(e) ensure that all network switches enable Private VLANs for segmented workstation networks to limit the ability of devices on a network to directly communicate with other devices on the subnet and limit an attacker's ability to laterally move to compromise neighbouring systems;

(f) ensure that all information stored within IT Environment shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principal that only authorized individuals should have

access to the information based on their need to access the information as a part of their responsibilities;

(g) ensure that sensitive information stored on the IT Environment shall be encrypted at rest and require a secondary authentication mechanism, not integrated into the operating system, in order to access the information;

(h) enforce detailed audit logging for access to non-public data and special authentication for sensitive data; and

(i) ensure that any archived data sets or systems that have not been accessed for 12 months shall be removed from the live environment. Such data sets or systems completely virtualized and powered off until needed and shall only be used as standalone systems (disconnected from the MoD Core Network) by the business unit needing to occasionally use the data set or system.

18.13 **SANS Control 18 – Application Software Security**

The Contractor shall apply NCSC guidance for secure development and deployment to the implementation of application software security by performing the following:

(a) ensure that for all acquired application software, check that the version you are using is still supported by the vendor. If not, update to the most current version and install all relevant patches and vendor security recommendations;

(b) protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks, including but not limited to cross-site scripting, SQL injection, command injection, and directory traversal attacks;

(c) for applications that are not web-based, deploy specific application firewalls if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed;

(d) ensure that for in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats;

(e) Test all in-house-developed and third-party-procured web applications for common security weaknesses using automated remote web application scanners prior to deployment, whenever updates are made to the application, and on a regular recurring basis. In particular, input validation and output encoding routines of application software should be reviewed and tested;

(f) ensure 'Output Sanitisation' by not displaying system error messages to End Users;

(g) maintain the Production Environments separate from any non-Production systems. Developers should not typically have unmonitored access to the Production Environment;

(h) for applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested;

(i) ensure that all software development personnel receive training in writing secure code for their specific development environment; and

(j) for in-house developed applications, ensure that development artefacts (sample data and scripts; unused libraries, components, debug code; or tools) are not included in the deployed software, or accessible in the production environment.

18.14 **SANS Control 19 – DART**

The Contractor shall record and maintain system application dependencies on the 'Defence Assurance Risk Tool' at all times.

18.15 **SANS Control 20 – Data Loss Prevention**

The Contractor shall:

(a) implement, promote, and enable data loss prevention at all times by utilising all available means within JPA and its associated applications to undertake end-to-end monitoring and data export attribution to individual account level. Such a solutions shall:

(i) be fully integrated into SOC and security technologies in order that 'normal' behaviours (as defined by the Authority) can be determined and monitored;

(ii) enable limits/constraints applied to prevent or mitigate 'abnormal' behaviour (as defined by the Authority); and

(iii) use meta-data to identify the type/nature of material populating any given field and, whenever a non-database document is saved, the requirement to set meta-data should be enforced utilising a taxonomy agreed with the Authority;

(b) undertake end-to-end monitoring and data export attribution, to individual account level by utilising greater technical data management to:

(i) define data types and locations;

(ii) define expected data flows;

(iii) enable data export (via printer or other electronic means) by authorised users to be monitored with a view to managing, controlling and if necessary limiting data export;

(iv) explore and if successful introduction of on screen messaging to warn users of the handling procedures required and possible consequences of exporting large volumes of sensitive personal data;

(v) fully integrate the SOC monitoring and security technologies develop and support DLP policies; and

(vi) define work flow and incident handling processes.

19 SECURITY AND INFORMATION GOVERNANCE

The Contractor shall provide support to the 'Security and Information Assurance Governance' structure by performing the following:

(a) coordinate, prepare and attend 'Security and Information Assurance Governance' meetings in coordination with the Authority (DBS ITS SO1 Sy) to schedule to be agreed with the Authority (DBS ITS SO1 Sy) on the Effective Date and reviewed annually. At each such meeting, the Contractor will be represented by the ASM and SMEs (as appropriate). These will include, but not be limited to, the following meetings:

(i) a 'Security Working Group' (SWG) meeting every 6 weeks or as required by the Authority;

(ii) a 'Assurance Strategy' meeting every 2 weeks or as required by the Authority;

(iii) a 'Security and IA Risk Review' meeting every prior to each SWG or as required by the Authority;

(iv) an 'ITSHC' routine and ad hoc meetings as agreed with the Authority (DBS ITS SO1 Sy); and

(v) an 'Information Asset Owners Working Group' meeting as required by the Authority (DBS).

APPENDIX 2: SECURITY MANAGEMENT PLAN

APPENDIX 3: S&PDAL