SCHEDULE 2.4

SECURITY MANAGEMENT

1. ORDER OF PRECEDENCE

1.1 Notwithstanding Clause 1.3, if there is a conflict between the provisions of this Schedule 2.4 (*Security Management*) and any other provisions of this Agreement in relation to security requirements and security management, this Schedule 2.4 (*Security Management*) shall prevail to resolve such conflict.

1.2 The Supplier shall comply with the Authority's security requirements contained within this Schedule 2.4 (*Security Management*) together with the provisions of Appendix B (Security Management Plan) of this Schedule 2.4 (*Security Management*) which sets out the Supplier's plan for managing security risks and responding to security requirements and Appendix D (Security and Data Protection) of this Schedule 2.4 (*Security Management*) which sets out the Supplier's solution with respect to security and data protection requirements. In the event of any conflict between the terms of this Schedule 2.4 (*Security Management*) and its Appendices, such conflict shall be resolved in accordance with the following order of precedence:

(a) Appendix A (Security Aspects Letter)

(b) Terms of Schedule 2.4 (*Security Management*)

(c) Appendix C (Cyber Risk Profile Security Requirements)

(d) Appendix B (Security Management Plan)

(e) Appendix D (Security and Data Protection).

2. DEFINITIONS

2.1 For the purposes of interpretation of this Schedule 2.4 (*Security Management*) the following expressions shall have the following meanings:

Administrator Responsibilities	means the Supplier Personnel given responsibility for carrying out functions which support the deployment or operation of a system within the IT Environment or a system account that is responsible for running a scheduled task periodically. In all cases, such individual will carry out functions that Supplier Personnel would otherwise not have access to and accordingly shall have a higher level of permissions in the IT Environment;
Alternative Security Controls	has the meaning given in Paragraph 11.2 of this Schedule 2.4 (*Security Management*);
Approve	means the Authority's prior written approval or consent, and "Approved" and "Approval" shall be construed accordingly;

Anti-Malicious Software	means software that scans for and identifies possible Malicious Software in the IT Environment;
Authority Matter	means any Classified Matter which is designated in writing by the Authority in a Security Aspects Letter, and shall include any information concerning the content of such matter and anything which contains or may reveal that matter;
Authority Property	means any property or assets owned by the Authority, including without limitation all documentation, software, firmware, databases, specifications, instructions, plans, processes, drawings, patterns, models, reports, designs, and any modifications to such material;
Authority Security Tests	has the meaning given in Paragraph 8.9;
Authority Site	means the location(s) occupied by the Authority and at which the Supplier is to perform the work or Services due under this Agreement or aspects of these;
Classified Matter	means any data, information, material, property or asset including without limitation any aspect of or matter connected with this Agreement or its performance which has a marking indicating the applicable protective security or privacy classification in accordance with the Security Policy Framework;
Cyber Essentials	means the Cyber Essentials scheme operated by the National Cyber Security Centre which defines a set of controls which, when properly implemented according to the relevant Cyber Risk Profile identified, will provide organisations with basic protection from the most prevalent forms of threat;
Cyber Improvement Plan	has the meaning given in Paragraph 4.3;
Cyber Risk Profile	means the risk profile given in relation to the Services following an assessment by the Authority (a risk level of N/A, Very Low, Low, Moderate or High as set out in Appendix C of this Schedule 2.4 (*Security Management*));
GSCP	means the Government Security Classification Policy published on 30 June 2023 by the Cabinet Office (or the latest version or iteration thereof), including any relevant accompanying guidance;

Higher Risk Sub-contractor	means each Sub-contractor classified as such by the Authority taking account of the sensitivity and scope of the data, information, material, property or asset affected;
Information Management System	means: (a) those parts of the Supplier System, including but not limited to those used on the Sites and remotely, that the Supplier or its Sub-contractors will use to provide the parts of the Services that require Processing Authority Data; and (b) the associated information assets and systems (including organisational structure, controls, policies, practices, procedures, processes and resources);
Low Risk Sub-contractor	means each Sub-contractor classified as such by the Authority taking account of the sensitivity and scope of the data, information, material, property or asset affected;
Moderate Risk Sub-contractor	means each Sub-contractor classified as such by the Authority taking account of the sensitivity and scope of the data, information, material, property or asset affected;
Need-to-know	Means access to Authority Data must be no wider than necessary for the efficient conduct of the Services, and limited to those with a business need and the appropriate personnel security clearance as set out in this Schedule 2.4 (*Security Management*);
Protective Monitoring System	has the meaning given in Paragraph 22.1 of this Schedule 2.4 (*Security Management*);
Relevant Conviction	means a conviction that is relevant to the nature of the Services or as listed by the Authority and/or relevant to the work of the Authority;
SaaS Sub-contractor	has the meaning given in Paragraph 22.6 of this Schedule 2.4 (*Security Management*);
Security Alerts	any events or occurrences which are identified during the Services and which would either increase the impact of a Security Breach or the probability that a Security Breach could occur;
Security Aspects Letter	means the Security Aspects Letter issued by the Authority for this Agreement or with any invitation to tender issued in respect of this Agreement to the

	Supplier and any further letter designated as such, issued by the Authority to the Supplier and contained at Appendix A to this Schedule 2.4 (*Security Management*), and which incorporates the Security Conditions contained at Annex A thereto;
Security Breach	means the occurrence of: (a) any unauthorised access to or use of the Services, the Authority Premises, the Sites, the Supplier System, the Authority System, the Information Management System and/or any information or data (including the Confidential Information and the Authority Data) used by the Authority, the Supplier or any Sub-contractor in connection with this Agreement; (b) the loss (physical or otherwise) and/or unauthorised disclosure of any information or data (including the Confidential Information and the Authority Data), including copies of such information or data, used by the Authority, the Supplier or any Sub-contractor in connection with this Agreement including the Authority Data; (c) any part of the Supplier System and/or Information Management System ceasing to be compliant with the Certification Requirements; (d) the installation of Malicious Software in the: (i) Information Management System; or (ii) IT Environment; (e) any loss of operational efficiency or failure to operate to specification as the result of the installation or operation of Malicious Software in the (i) Information Management System; or (ii) IT Environment; (f) includes any attempt to undertake the activities listed in sub-paragraph (a) where the Supplier has reasonable grounds to suspect that attempt:

	(i) was part of a wider effort to access information and communications technology operated by or on behalf of Central Government Bodies; or (ii) was undertaken, or directed by, a state other than the United Kingdom; and (g) to the extent not already covered by (a)-(f) above, a Data Loss Event;
Security Conditions	means the requirements set out in Annex A to the Security Aspects Letter;
Security Lead	means the role described in Paragraph 6 of this Schedule 2.4 (*Security Management*);
Security Management Plan	means the Supplier's security plan based on the template provided at Appendix B of this Schedule 2.4 (*Security Management*) and as subsequently developed and revised pursuant to Paragraphs 8 and 9 of this Schedule 2.4 (*Security Management*);
Security Policy Framework	means the HMG Security Policy Framework as amended or up-dated from time to time which is issued by the Cabinet Office;
Security Working Group	has the meaning given in Paragraph 23 of this Schedule 2.4 (*Security Management*);
Supplier Assurance Questionnaire	means the risk assessment process which is used to measure the Cyber Risk Profile for this Agreement and any Sub-contract;
Supplier Site	means those premises of the Supplier at which work or Services are being performed under this Agreement or at which Authority Data or Classified Matter is held;

2.2 In this Schedule 2.4 (*Security Management*), unless a contrary intention is expressly set out, all other capitalised terms shall have the same meaning as is set out in this Agreement.

3. CONSEQUENCES OF BREACH

3.1 The Supplier shall (and shall ensure its Supplier Personnel and Sub-contractors) comply with the security requirements specified in this Schedule 2.4 (*Security Management*).

3.2 The Supplier shall (and shall procure that its Supplier Personnel and Sub-contractors) comply with any additional security provisions set out in an applicable Security Aspects Letter.

3.3 Any breach of the security requirements specified in this Schedule 2.4 (*Security Management*) may constitute a Security Breach and have implications for continued access to the Authority Sites and security clearance.

3.4 The decision of the Authority as to whether any person is to be refused access to the Authority Site and as to whether the Supplier has failed to comply with the relevant site access security provisions shall be final and conclusive.

3.5 A decision of the Authority on the question of whether the Supplier has taken or is taking reasonable steps as required by this Schedule 2.4 (*Security Management*) shall be notified to the Supplier and shall be final and conclusive.

3.6 Any material breach of a provision of this Schedule 2.4 (*Security Management*) (which can be one incident or failure or a series of incidents or failures depending on the impact or potential impact) shall entitle the Authority to terminate this Agreement for cause.

4. CYBER RISK PROFILE

4.1 The Authority has determined the Cyber Risk Profile appropriate to this Agreement and has notified the Supplier of that Cyber Risk Profile, and shall notify the Supplier as soon as reasonably practicable where the Authority reassesses the Cyber Risk Profile relating to this Agreement.

4.2 Once the Supplier has been notified of the Cyber Risk Profile appropriate to this Agreement in accordance with Paragraph 4.1 (including a change of Cyber Risk Profile following an Authority reassessment), the Supplier shall, and shall procure that its Sub-contractors shall, ensure that the requirements relevant to the assessed Cyber Risk Profile, as set out in Appendix C of this Schedule 2.4 (*Security Management*), are followed.

4.3 The Supplier shall ensure that a risk assessment is completed with respect to both the Supplier and each Sub-contractor in accordance with DEFSTAN 05-138 and a Cyber Risk Profile determined, and shall, and shall procure that its Sub-contractors shall, complete a Supplier Assurance Questionnaire for the assigned Cyber Risk Profile:

(a) within one (1) month of the Effective Date;

(b) no less than once in each year of this Agreement commencing on the first anniversary of completion of the first Supplier Assurance Questionnaire at Paragraph 4.3(a) above;

(c) where a change is proposed to:

(i) the Supplier's supply chain; and/or

(ii) the Supplier's Security Management Plan at Appendix B of this Schedule 2.4 (*Security Management*),

in both cases such as has or may have an impact on the Cyber Risk Profile with the impact being agreed by the Parties, acting reasonably; and

(d) at any other time upon receipt of any reasonable request to do so by the Authority; and

should the Supplier or any of its Sub-contractors fail to meet the required Cyber Risk Profile requirements, a Cyber Improvement Plan must be completed and submitted to the Authority for its approval and shall detail areas in which improvements are needed by the Supplier and/or Sub-contractor in order to successfully meet the Cyber Risk Profile requirements, together with a plan of action for making such improvements within agreed time limits.

5. CERTIFICATION REQUIREMENTS

5.1 The Supplier shall ensure that, as an organisation, it is certified as compliant with:

(a) ISO/IEC 27001:2022 by a United Kingdom Accreditation Service-approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001:2022; and

(b) Cyber Essentials Plus,

and shall provide the Authority with a copy of each such certificate of compliance before the Supplier shall be permitted to receive, store or Process Authority Data.

5.2 The Supplier shall ensure that each Higher Risk Sub-contractor is, as an organisation, certified as compliant with either:

(a) ISO/IEC 27001:2022 by either a United Kingdom Accreditation Service-approved certification body or, where agreed by the Authority, an equivalent non-UK certification body, or is included within the scope of an existing certification of compliance with ISO/IEC 27001:2022; or

(b) Cyber Essentials Plus,

and shall provide the Authority with a copy of each such certificate of compliance before the Higher-Risk Sub-contractor shall be permitted to receive, store or Process Authority Data.

5.3 The Supplier shall ensure that each Sub-contractor classified as a Low Risk Sub-contractor or a Moderate Risk Sub-contractor is certified compliant with Cyber Essentials Plus, although this requirement shall be deemed met if the relevant Sub-contractor is certified compliant with either certification described at Paragraph 5.2(a) and 5.2(b).

5.4 Subject also to the requirements of paragraph 33 of the Security Conditions, the Supplier shall ensure that the Supplier and each Sub-contractor who is responsible for the secure destruction of Authority Data:

(a) should satisfy the Authority that their data destruction/ deletion practices comply with UK GDPR requirements and follows all relevant UK Government

and NCSC guidance or, by exception, such other equivalent guidance as has been agreed with the Authority;

(b) are, where certification applies, certified as compliant with the NCSC Assured Service (CAS) Service Requirement Sanitisation Standard or an alternative standard as agreed by the Authority; and

(c) must maintain an asset register of all Authority supplied information, data and equipment to ensure Authority Assets are returned and/or deleted.

5.5 The Supplier shall provide the Authority with evidence of its and its Sub-contractor's compliance with the requirements set out in this Paragraph 5 before the Supplier or the relevant Sub-contractor (as applicable) may carry out the secure destruction of any Authority Data.

5.6 The Supplier shall notify the Authority as soon as reasonably practicable and, in any event within two (2) Working Days, if the Supplier or any Sub-contractor ceases to be compliant with the Certification Requirements, such notification including details of:

(a) why the Certification Requirements cannot be met;

(b) the potential impact of such Certification Requirements not being met on the Services and compliance by the Supplier and/or relevant Sub-contractor with this Schedule 2.4 (*Security Management*); and

(c) a proposed plan with respect to rectification of such non-compliance.

5.7 With respect to an occurrence of non-compliance with Certification Requirements as described at Paragraph 5.6 above, upon request from the Authority, the Supplier shall or shall procure that the relevant Sub-contractor shall:

(a) immediately ceases using the Authority Data or, where unfeasible to do so, work with the Authority to agree an urgent timetable for ceasing the use of Authority Data; and

(b) procure that the relevant Sub-contractor promptly returns, destroys and/or erases the Authority Data in accordance with the requirements set out in this Paragraph 5.

5.8 The Authority may agree to exempt, in whole or part, the Supplier or any Sub-contractor from the requirements of this Paragraph 5. Any exemption must be in writing to be effective. The Supplier must include the exemption in the Security Management Plan.

6. SECURITY LEAD

Appointment and role of Security Lead

6.1 The Supplier's Security Lead shall act as the Supplier's initial point of contact for all security issues between the Supplier and the Authority. The Supplier will inform the Authority of the Security Lead's contact details.

6.2 The Security Lead shall handle all elements of security with regard the work undertaken by the Supplier for the Authority and in all dealings with the Authority with regards to security matters.

6.3 The Security Lead is responsible for interpreting, implementing and monitoring the security controls necessary to provide the appropriate degree of protection in line with the level of protective marking applied by any applicable Security Aspects Letter and for ensuring that Supplier Personnel are aware of and adhere to the Authority's security requirements set out in this Schedule 2.4 (*Security Management*).

Training of Security Lead

6.4 If the Authority, acting reasonably considers that the Security Lead's current qualifications are inadequate for the Security Lead role, then the Authority and the Supplier will discuss how to rectify this. If the Authority and the Supplier cannot agree on how to improve the Security Lead's qualifications then the Authority may request that a different person is appointed to the role of Security Lead, in which case the Supplier shall promptly action this request.

7. COMPLIANCE WITH THE SECURITY POLICY FRAMEWORK AND THE GOVERNMENT SECURITY CLASSIFICATION POLICY (GSCP)

7.1 The Supplier shall (and shall procure that its Supplier Personnel and Sub-contractors shall) at all times:

(a) provide a level of security which complies with the security requirements, measures and standards set out in the Security Policy Framework;

(b) follows the guidelines relating to the treatment of Classified Material in the GSCP; and

(c) complies with the Security Aspects Letter at Appendix A to this Schedule 2.4 (*Security Management*).

7.2 At the request of the Authority, the Supplier shall confirm to the Authority that the Supplier's security measures are consistent with this Schedule 2.4 (*Security Management*), the Security Policy Framework and the GSCP. Any inconsistency or non-compliance with the Security Policy Framework, GSCP or Security Aspects Letter shall be notified to the Authority immediately and shall be addressed dependent on the severity of such inconsistency or non-compliance either at a regular meeting of the Security Working Group or by calling an emergency Security Working Group meeting, as the Parties shall, acting reasonably, agree.

7.3 The Authority shall be entitled to all such information as it may reasonably require to be satisfied that the Supplier, Supplier Personnel and any Sub-contractors (where applicable) are complying with the obligations set out in this Schedule 2.4 (*Security Management*).

7.4 The Supplier shall ensure that any information received marked as OFFICIAL or above from or held about the Authority pursuant to this Agreement, is held in a secure fashion in accordance with HMG policy and in particular the GSCP, including locking material away so that only appropriately security-cleared Supplier Personnel can access such material, and using encryption software on all computers (apart from computers, such as servers located in dedicated machine rooms, that are subject to adequate physical and procedural access controls) and portable media devices.

8. SECURITY MANAGEMENT PLAN

8.1 Within twenty (20) Working Days from the Effective Date, the Supplier shall, at its own cost, prepare and deliver to the Authority for the Authority's written approval a draft Security Management Plan aligning to the requirements set out in Appendix B of this Schedule 2.4 (*Security Management*) which it shall implement, operate and maintain (in accordance with continuous improvement principles) and shall be in accordance with this Schedule 2.4 (*Security Management*) and shall apply during the Term.

8.2 Following receipt of the draft Security Management Plan from the Supplier, the Authority:

(a) shall review and comment on the draft Security Management Plan as soon as reasonably practicable;

(b) may request that the Supplier attends a workshop (or a series of workshops) so that the Parties (acting reasonably) can work through the Supplier's draft Security Management Plan in collaboration, answering and working to resolve any Authority questions or issues ("**SMP Workshop**"); and

(c) shall notify the Supplier in writing that it approves or rejects the draft Security Management Plan no later than twenty (20) Working Days after the date on which the draft Security Management Plan is first delivered to the Authority or, in the case of a SMP Workshop having been arranged as per Paragraph 8.2(b) above, no later than ten (10) Working Days following completion of the final workshop.

8.3 If the Authority rejects the draft Security Management Plan:

(a) the Authority shall inform the Supplier in writing of its reasons for its rejection and may invite the Supplier to attend another SMP Workshop in order to work through the reasons for its rejection and work with the Supplier, collaboratively, to resolve such reasons; and

(b) the Supplier shall then revise the draft Security Management Plan (taking reasonable account of the Authority's comments) and shall re-submit a revised draft Security Management Plan to the Authority for the Authority's approval either within ten (10) Working Days of the date of the Authority's notice of rejection or, in the case of a SMP Workshop being held as per Paragraph 8.3(a) above, five (5) Working Days following completion of the final workshop. The provisions of Paragraph 8.2 and 8.3 shall apply again to any resubmitted draft Security Management Plan, provided that either Party may refer any disputed matters for resolution by the Dispute Resolution Procedure.

8.4 The approved Security Management Plan shall be incorporated at Appendix B of this Schedule 2.4 (*Security Management*) and shall be reviewed in line with Part 9 below.

8.5 The Supplier shall fully comply with its obligations set out in the Security Management Plan.

8.6 The Security Management Plan shall, unless otherwise specified by the Authority in this Schedule 2.4 (*Security Management*), aim to protect all aspects of the Services and all systems, processes, and sites associated with provision of the Services where the Supplier has responsibility, and shall specify and at all times comply with such security measures and procedures as are sufficient to ensure compliance with the provisions of this Schedule 2.4 (*Security Management*).

8.7 The Security Management Plan shall be written in plain English, in language which is readily comprehensible to the staff of the Supplier and the Authority engaged in the Services, and shall only reference documents which are in the possession of the Authority or whose location is otherwise specified in this Schedule 2.4 (*Security Management*).

8.8 The Security Management Plan shall fully detail the security measures and relevant security terms and conditions, measures, standards and policies of any relevant Sub-contractor, as detailed at Paragraph 18.3(b) below.

8.9 The Authority and/or its authorised representatives shall be entitled, at any time and without giving notice to the Supplier, to carry out such tests (including penetration tests and other forms of ethical hacking) as it may deem necessary in relation to the Service, the Information Management System and/or the Supplier's compliance with the Security Management Plan (**"Authority Security Tests"**). The Authority shall take reasonable steps to notify the Supplier prior to carrying out such Authority Security Test to the extent that it is reasonably practicable for it to do so taking into account the nature of the Authority Security Test, and the Authority Security Tests shall be designed and implemented so as to minimise their impact on the delivery of the Services.

9. AMENDMENT AND REVISION OF THE SECURITY MANAGEMENT PLAN

9.1 The Security Management Plan will be reviewed and updated by the Supplier as required, and at least annually, to reflect:

(a) emerging changes in relevant guidance and policy including but not limited to Authority or wider HM Government policies and guidance, Good Industry Practice, the Security Policy Framework and the GSCP;

(b) any change or proposed change to the Supplier's systems and processes, and the Supplier Services and/or associated processes;

(c) any change or proposed change to any relevant Sub-contractor's systems and processes including any security terms and conditions, measures, standards and policies;

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

(e) any reasonable request by the Authority, including where such requests arise from the results of an Authority Security Test, with such proposed updates being dealt with as a Contract Change under Schedule 8.2 (*Change Control Procedure*) where the Parties, acting reasonably, consider it appropriate to do so;

and the Authority shall be entitled, acting reasonably, to request a more frequent review of the Security Management Plan upon the occurrence of any of (a) - (e) above.

9.2 The Supplier shall provide the Authority with the written results of such reviews as soon as reasonably practicable after their completion and amend the Security Management Plan at no additional cost to the Authority. The results of the review shall include:

(a) any proposed modifications to the procedures and controls that are covered by the Security Management Plan; and

(b) any proposed improvements in measuring the effectiveness of these procedures and controls.

9.3 On receipt of the results of such reviews, the Authority will decide whether or not to Approve any amendments or revisions to the Security Management Plan proposed by the Supplier. The Authority may also propose further changes to the Security Management Plan on receipt of the results of such reviews.

9.4 Any change or amendment which the Supplier proposes to make to the Security Management Plan shall be subject to the change control procedure under this Agreement and reflected in Part 12 of the Security Management Plan, and shall not be implemented until Approved by the Authority.

10. OFFICIAL-SENSITIVE INFORMATION

10.1 For the purposes of this Paragraph, "**Information**" means information recorded in any form disclosed or created in connection with this Agreement.

10.2 The Supplier shall protect all Information relating to the aspects designated OFFICIAL-SENSITIVE as identified in the Security Aspects Letter, and in accordance with the official security conditions contained in this Agreement.

10.3 The Supplier shall include the requirements and obligations set out in Paragraphs 10.2 and 18.3 in any Sub-contract placed in connection with or for the purposes of this Agreement which requires disclosure of OFFICIAL-SENSITIVE Information to the Sub-contractor or under which any Information relating to aspects designated as OFFICIAL-SENSITIVE is created by the Sub-contractor. The Supplier shall also include in the Sub-contract a requirement for the Sub-contractor to flow the requirements of this Paragraph 10 to its Sub-contractors and through all levels of the supply chain to the lowest level where any OFFICIAL-SENSITIVE Information is handled.

11. SUPPLIER PERSONNEL

Vetting

11.1 Subject to Paragraph 11.2 below, the Supplier shall ensure that all Supplier Personnel shall:

(a) except where Supplier Personnel are subject to Paragraph 11.1(b) below, be vetted to the standards of BPSS (Baseline Personnel Security Standard) as per paragraph 11 of the Security Conditions;

(b) in the case of those having Administrator Responsibilities, have additional vetting applied to them to SC (Security Checks) standards; and

(c) subject to Paragraph 11.5 below:

(i) be the subject of an appropriate level of personnel security checks, where the BPSS is applied as a minimum;

(ii) be given appropriate initial and ongoing security education, training and awareness; and

(iii) be familiar with and signed up to the security operating procedures governing the use of relevant systems and are aware of local processes for reporting issues of security concern.

11.2 The requirements of 11.1(a)-(c) above shall apply to all Supplier Personnel unless other alternative security controls have been agreed with the Authority dependant on the relevant user role, capability and data access, such agreement being in the absolute discretion of the Authority (**"Alternative Security Controls"**).

Security Clearance

11.3 It is a condition of this Agreement that all Supplier Personnel shall have any checks or security clearances as stipulated in the Security Aspect Letter, in addition to the vetting requirements set out above, unless Alternative Security Controls have been agreed with the Authority.

11.4 Without prejudice to any other provision of this Agreement, where any member of Supplier Personnel or Sub-contractors has been involved in a material (where "material" involves a Security Breach involving OFFICIAL-SENSITIVE and/or Authority Data) Security Breach (or where the Authority has reasonable grounds for suspecting that such an individual has been involved in a material Security Breach), the Authority may request the Supplier to promptly ensure the relevant individual is suspended from involvement in any work in connection with this Agreement while the extent of the individual's involvement in the Security Breach is being investigated. Depending on the outcome of that investigation, the Supplier and the Authority may or may not then agree that the individual's suspension from any work in connection with this Agreement should be made permanent.

11.5 If the Supplier is permitted to commence performance of this Agreement prior to certain Supplier Personnel obtaining security clearance and such security clearance is subsequently not obtained by the relevant Supplier Personnel, the Authority shall be entitled to summarily terminate the engagement of the relevant individual who has failed to gain the necessary level of clearance as required by the Authority.

11.6 In relation to personnel vetting and security clearances, the decisions of National Security Vetting (NSV) shall be final and binding on the Parties.

Compliance with Security

11.7 The Supplier shall ensure that all Supplier Personnel are aware of, understand and adhere to all relevant security rules at all times, and where necessary, undergo further security induction, such obligation including the responsibilities of the Security Lead outlined at Paragraph 6.3 above.

11.8 The Supplier shall ensure that its Supplier Personnel are aware of, understand and adhere to all relevant standard national rules relating to the handling, transmission, storage and destruction of Classified Matter as detailed in the Security Management Plan.

11.9 The Supplier shall inform and ensure Supplier Personnel that they must abide by all of the Authority's security requirements as detailed in this Agreement (including this Schedule 2.4 (*Security Management*)) or as advised to the Supplier by the Authority on an ongoing basis.

Conduct of Supplier Personnel

11.10 Supplier Personnel must not engage in any conduct which would or might discredit or cause embarrassment to or reduce the effectiveness of or weaken confidence in the integrity of the Authority and, further, when working on an Authority Site, must adhere to such of the Authority's policies and codes of conduct related to that Authority Site as are communicated to them from time to time including (but not limited to) those relating to security, health and safety, the communications systems and equal opportunities.

11.11 The Authority has a zero-tolerance policy towards the illegal use or possession of drugs. The Supplier must inform all Supplier Personnel of the aforementioned Authority's policy.

11.12 The Supplier shall ensure that no person who discloses that he/she has a Relevant Conviction, or is found by the Supplier to have a Relevant Conviction (whether as a result of a police check or through a Criminal Records Bureau check or otherwise) is employed or engaged in the provision of any part of the Services.

11.13 The Supplier acknowledges and will inform Supplier Personnel that the use of the Authority's systems and devices which they may have occasion to use during the course of their daily business with the Authority will be monitored.

11.14 Where there are reasonable concerns related to the security clearance and/or conduct of any Supplier Personnel and/or any person employed or engaged by any member of Supplier Personnel, the Authority may:

(a) remove and exclude them from the Authority Sites;

(b) instruct the Supplier to remove them from the provision of Services to the Authority;

(c) quarantine any of their personal effects on the Authority Sites to help facilitate an internal security investigation; and

(d) take such other security measures as may be necessary to assess and limit damage to the Authority's business, operations and reputation.

Travel Restrictions

11.15 The Security Lead must inform and brief all relevant Supplier Personnel for whom Alternative Security Controls have been agreed that they must notify him/her, giving reasonable notice, in the event that they intend to travel to any country defined by the Authority as a security risk, for example CSSTRA nations, or that is otherwise advised by the Authority, during the time they provide Services to the Authority under this Agreement, except that in the case of SaaS Sub-contractor personnel, the Authority, acting in its absolute discretion, may agree that making such notification is not practicable in the circumstances and agree that alternative means of ensuring compliance with this Paragraph 11.15 can be used. Those Supplier Personnel granted SC or DV clearance must, with respect to travel to such countries defined by the Authority as a security risk, follow the relevant rules relating to travel aligning to the clearance level granted.

11.16 Upon receiving a notification as described at Paragraph 11.15 above, the Security Lead will promptly notify the Authority of any such proposed visit by the Supplier Personnel to any country defined by the Authority.

11.17 The Authority may make representations to the Supplier that the proposed visit must not take place if, in the view of the Authority, this is vital to protect the interests of national security or the individual. The resolution on this matter will be agreed between the Authority and Supplier.

Miscellaneous provisions

11.18 The Supplier Personnel shall not hold himself out, and has no authority, unless such is expressly conferred in writing by the Authority, to hold himself out to any third person as an employee or agent of the Authority.

11.19 The Supplier shall bear the cost of any notice, instructions or decision of the Authority under this Paragraph 11 except where agreed pursuant to the Change Control Procedure.

12. AUTHORITY SITES

Access to the Authority Sites

12.1 In addition to Paragraphs 11.14 and 12.9, the Authority may, at any time, refuse to admit onto, or withdraw permission to remain on, the Authority Site:

(a) any member of Supplier Personnel; or

(b) any person employed or engaged by any member of Supplier Personnel,

whose admission or continued presence would, in the sole opinion of the Authority, be undesirable.

12.2 The Supplier, its Supplier Personnel and/or any person employed or engaged by any member of Supplier Personnel shall only attend the Authority Site on the express invitation of the Authority, and where such attendance is necessary for the provision of the Services under this Agreement, and for no other reason.

12.3 The Supplier shall provide a list of the names and addresses of all Supplier Personnel and/or any person employed or engaged by any member of Supplier Personnel who may require admission in connection with this Agreement to the Authority Site, specifying the capacities in which they are concerned with this Agreement and giving such other particulars as the Authority may reasonably request.

12.4 The Supplier shall comply (and shall ensure its Supplier Personnel and/or any person employed or engaged by any member of Supplier Personnel comply) with all rules, regulations, requirements and policies (including those relating to security arrangements) as may be in force from time to time for the conduct of personnel when at or outside the Authority Site. The Supplier Personnel and/or any person employed or engaged by any member of Supplier Personnel shall ensure that they familiarise themselves with all such rules, regulations, requirements and policies which they will be instructed by the Authority on where to find. It is the ongoing responsibility of the Supplier Personnel and/or any person employed or engaged by

any member of Supplier Personnel to ensure they are in compliance with Authority rules, regulations, requirements and policies as these are made known to the Supplier by the Authority.

12.5 Only Supplier Personnel and/or any person employed or engaged by any member of Supplier Personnel who have been appropriately security cleared and authorised by the Authority shall have access to the Authority Sites.

12.6 Supplier Personnel and/or any person employed or engaged by any member of Supplier Personnel shall only access those areas of the Authority Sites necessary for the direct provision or management of work or services provided under this Agreement and to which their passes allow access. Supplier Personnel and/or any person employed or engaged by any member of Supplier Personnel shall not intentionally attempt to access any other area of any Authority Site except at the Authority's invitation or if necessary for evacuation in the event of a genuine emergency. Where Supplier Personnel and/or any person employed or engaged by any member of Supplier Personnel are permitted access to other parts of the Authority Sites, they must be accompanied at all times by a member of the Authority staff.

Passes

12.7 Supplier Personnel may be issued with a pass if so required which is expected to be permanent or time bound (and which, for the avoidance of doubt, is not a temporary or day pass). This pass must be worn and visible at all times whilst on any Authority Site. This pass must be kept and used in accordance with the Authority instructions notified from time to time. Such pass will indicate whether or not the holder is granted unescorted access to a given Authority Site.

12.8 Other Supplier Personnel who are not eligible to be issued with a pass shall be escorted about the Authority Site in accordance with the Authority policies. The Authority may also require Supplier Personnel with a pass to be escorted about the Authority Site.

12.9 Supplier Personnel who cannot produce a valid pass when required to do so or who contravene any instructions on the basis of which a pass was issued, may be required to leave and refused further admission to the Authority Sites.

12.10 The passes are official documents covered under the Official Secrets Acts and their loss must be reported to the Authority. The passes must remain in the United Kingdom (UK) at all times; taking or sending them out of the UK is not permitted under any circumstances. If a pass is stolen in the UK, the theft should also be reported to the police, a crime number obtained and supplied to the Authority.

12.11 Repeated incidents of loss of or damage to an Authority pass by a member of Supplier Personnel shall constitute a security breach and may have implications for their continued access to the Authority Sites and their security clearance.

12.12 The Security Lead must inform the Authority of anyone who is leaving the employment of the Supplier or ceasing to be contracted to the Supplier (or one of its contractors) or ceasing to have involvement under this Agreement and who has been issued with an Authority pass so that the pass may have its access switched off and

the staff file amended accordingly. The pass must also be returned in a secure manner to the Authority for its destruction as soon as is practically possible.

Restrictions on the introduction of portable equipment onto the Authority Sites

12.13 Supplier Personnel must seek guidance on and comply with the Authority's security procedures (as notified to the Supplier by the Authority or prominently displayed at the relevant Authority Sites) if they need to bring in or take out any of the following from the Authority Sites:

(a) mobile phones, PDAs or other Personal Electronic Devices (PEDs);

(b) tape recorders or similar oral recording devices;

(c) cameras, any item with a built-in camera or any other visual recording devices;

(d) any item with wireless connectivity (Bluetooth, Wi-Fi etc.), transmitting or receiving capability;

(e) fixed or removable media of any form, including: CDs, DVDs, HDDs, videos, cassette tapes, USB storage devices, removable memory cards etc., whether held as a separate item or within another device;

(f) any items of wearable technology; or

(g) laptops, netbooks and removable hard disks.

12.14 The Authority reserves the right to permanently confiscate items covered under Paragraph 12.13 if they are discovered on an Authority Site without the appropriate authorisation being in place.

Restrictions on the removal of business materials from the Authority Sites

12.15 The Supplier shall not remove (or cause to be removed) and re-use any equipment from an Authority Site that contains any electronic memory retaining components that have at any stage been connected to the Authority systems unless they have first obtained the Authority's express written permission to do so.

12.16 Any equipment used at any time on the Supplier Site that contains the Authority Data shall be purged of all Authority Data at the end of this Agreement unless specifically told otherwise, and it shall be the responsibility of the Supplier to ensure that all such data is completely and effectively purged, with confirmation of the same being provided by the Supplier to the Authority upon completion (this being no later than 30 (thirty) Working Days after the termination of this Agreement).

Restrictions on the introduction or removal of Classified Matter from the Authority Sites

12.17 The Supplier shall ensure that Supplier Personnel comply fully with the requirements relating to OFFICIAL and OFFICIAL-SENSITIVE materials and equipment as outlined at paragraphs 4 to 25 of the Security Conditions.

Searches of bags, cases and packages carried by Supplier Personnel

12.18 When entering or leaving an Authority Site, Supplier Personnel, in common with the Authority's staff, may be required to submit any bags, cases, and packages carried for searching by the Authority's security officials. Detection of the unauthorised import or export of any of the items listed in Paragraphs 12.13, 12.15, 12.17 or paragraphs 22 to 25 (inclusive) of the Security Conditions onto or off the Authority's estate shall constitute a security breach; the item shall be confiscated and this may have implications for continued access to the Authority Sites and security clearance.

Use of the Authority System by Supplier Personnel

12.19 Use of the Authority's System is conditional upon adherence to security operating procedures and any local security instructions or policies enforced by the Authority. Supplier Personnel will be advised which aspect of the Authority System they will need to use during business discussions with their Authority sponsors and which security operating procedures or local security policies apply. Supplier Personnel must abide by security operating procedures governing the Authority System at all times.

12.20 The Supplier shall (and shall ensure that the Supplier Personnel shall) abide by the security operating procedures or policies of the Authority System and Authority Data, and shall not attempt to gain unauthorised access to the Authority System and/or Authority Data which is not essential for the provision of the work or Services under this Agreement.

13. AUTHORITY MATTER

13.1 Unless it has the written authorisation of the Authority to do otherwise, neither the Supplier nor any Supplier Personnel shall, either before or after the completion or termination of this Agreement, do or permit to be done anything which they know or ought reasonably to know may result in Authority Matter being disclosed to or acquired by a person in any of the following categories:

(a) who does not hold the appropriate authority (including relevant security clearance Approved by the Authority (subject to Paragraph 11.6)) for access to the protected matter;

(b) in respect of whom the Authority has notified the Supplier in writing that the Authority Matter shall not be disclosed to or acquired by that person;

(c) who is not a member of Supplier Personnel; and

(d) who is a member of Supplier Personnel but has no need to know the information for the proper performance of this Agreement (as described in paragraph 10 of the Security Conditions).

13.2 Unless it has the written permission of the Authority to do otherwise, the Supplier and Supplier Personnel shall, both before and after the completion or termination of this Agreement, take all reasonable steps to ensure that:

(a) no photograph of, or pertaining to, any Authority Matter shall be taken and no copy of or extract from any Authority Matter shall be made except to the extent necessary for the proper performance of this Agreement; and

(b) any Authority Matter upon request, is delivered up to the Authority who shall be entitled to retain it.

14. ELECTRONIC ACCESS

14.1 Electronic access to IT systems on which the Authority Property, Authority Data and/or any Classified Matter is held shall be controlled in accordance with the Security Policy Framework and/or the GSCP, paragraphs 18 to 21 (inclusive) of the Security Conditions and additional rules for specific systems such as MODNet rules for MODNet access.

14.2 IT systems on which Authority Property, Authority Data and/or Classified Matter are held must have been approved following the Secure by Design process which shall be determined by the Authority and agreed with the Supplier.

14.3 Electronic access to the IT systems on which the Authority Property, Authority Data and/or Classified Matter is held shall only be allowed to authorised Supplier Personnel with the appropriate security clearance (as determined and Approved by the Authority) and subject to paragraph 5 of the Security Aspects Letter and paragraph 21.a of the Security Conditions.

15. COMMUNICATIONS SECURITY AT SUPPLIER SITES

15.1 The Supplier Security Lead shall ensure that all communications from the Supplier Site to the Authority Sites, whether written, by telephone, by electronic data transfer or by employing removable IT media, comply with the terms set out in the Security Policy Framework, the GSCP and paragraphs 14 to 17 (inclusive) of the Security Conditions.

15.2 To assist in secure telephone and IT communications between the two (2) Parties, the Authority may choose to install or sponsor the installation of secure telephones and a secure means to transmit Classified Matter and Authority Data at the Supplier Sites.

15.3 If Paragraph 15.2 applies, then the appropriate physical and procedural security will be required to be in place to protect the equipment. Any changes will be undertaken subject to change control.

16. TECHNICAL ACCESS

16.1 The Supplier shall ensure that a log is maintained of all electronic access to computer and IT systems which have been used to conduct the Authority business and/or have been used to process and store the Authority Data.

16.2 Upon request by the Authority, the Supplier shall provide these records to the Authority.

17. SECURITY BREACHES AND SECURITY INVESTIGATIONS

17.1 If either Party becomes aware of a Security Breach it shall notify the other as soon as reasonably practicable after becoming aware of the breach, and in any event within twenty-four (24) hours.

17.2 The Supplier must, upon becoming aware of a Security Breach immediately take those steps identified in the Security Management Plan (if applicable) and all other steps reasonably necessary (which shall include any action or changes reasonably required by the Authority which shall be completed within such timescales as the Authority may reasonably require) to:

(a) minimise the extent of actual or potential harm caused by such Security Breach;

(b) remedy such Security Breach to the extent possible and protect the integrity of the Information Management System and/or the Supplier System against any such potential or attempted Security Breach;

(c) apply a tested mitigation against any such Security Breach and, provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier's ability to deliver the Services so as to meet any Performance Indicator, the Supplier shall be granted relief against the failure to meet such affected Performance Indicator for such period as the Authority, acting reasonably, may specify by written notice to the Supplier; and

(d) prevent a further Security Breach in the future exploiting the same root cause failure;

17.3 and provide the Authority with regular updates (the regularity of which shall be appropriate to the severity of the Security Breach) providing the Authority with full details of the Security Breach as known to the Supplier at that time, together with evidence of all actions taken at that time in response to the Security Breach and including, where possible, a root cause analysis.

17.4 In the event that any action is taken in response to a Security Breach which occurred as a result of non-compliance of the Information Management System and/or the Security Management Plan with the requirements of this Agreement, then such action and any required change to the Information Management System and/or Security Management Plan shall be completed by the Supplier at no cost to the Authority.

17.5 If the Supplier fails to comply with its obligations set out in this Paragraph 17, such failure shall constitute a material Default, which if not remedied to the satisfaction of the Authority, shall permit the Authority to terminate this Agreement with immediate effect by issuing a Termination Notice to the Supplier.

17.6 A Security Breach has the ability, in differing categories of severity, to have an adverse impact on the secure discharge of the Authority's business and operations. A severe Security Breach or repeated Security Breaches by an individual may result in the loss of their security clearance.

17.7 Security Breaches are closely associated with the protection of Classified Matter or Authority Data. Therefore:

(a) disclosure of Classified Matter or Authority Data by the Supplier or Supplier Personnel to any persons who are not known to hold an appropriate security clearance or who have no Need-to-know the information in question shall be regarded as a Security Breach and shall be reported to the Authority through the Security Lead immediately. If at any time either before or after the completion or termination of this Agreement, the Supplier or any member of the Supplier Personnel discovers or suspects that an unauthorised person is seeking or has sought to obtain any Classified Matter or Authority Data, the Supplier shall immediately inform the Authority of the matter with full particulars;

(b) the Supplier and its agents and employees shall not assume that immunity will be granted from penalties under UK law for the unauthorised disclosure of Classified Matter (wherever that disclosure takes place) by virtue of the Parties executing this Agreement; and

(c) should any Security Breach occur at any Supplier Site, the Supplier shall notify the Authority and shall immediately investigate and report on the cause of the breach, including planned corrective action. Where directed by the Authority, the Supplier shall correct or repair the problems that gave rise to or facilitated the Security Breach.

17.8 The Authority reserves the right to initiate an investigation and containment exercise at the Supplier Site in response to the discovery of a Security Breach at such Supplier Site, unless, following best endeavours by the Supplier to facilitate such an investigation and containment exercise, the Authority acting in its absolute discretion agrees that initiating such investigation and containment exercise is not practicable in the circumstances and agrees that alternative means of investigating and containing the Security Breach can be used.

17.9 The Supplier, and the Security Lead in particular, shall cooperate with any investigation relating to security which the Authority carries out howsoever it may originate.

17.10 Where unusual Security Alerts are presented by the Supplier's programme team to the Supplier's Security Lead, if deemed pertinent by the Security Lead, the Authority shall be notified and shall be notified of the Security Lead's recommendation. The Parties shall comply with any requirements and timeframes imposed by the Authority's Warning and Reporting Point (WARP) in relation to Security Incidents.

18. SUB-CONTRACTS

18.1 All references to Supplier Personnel and Supplier Sites in this Schedule 2.4 (*Security Management*) also include the personnel and sites of any Sub-contractor which the Supplier may be permitted to use in performing work and Services under this Agreement.

18.2 Sub-contracting any part of this Agreement shall not relieve the Supplier of any of its obligations or duties under this Agreement. The Supplier shall be responsible for the acts and omissions of its Sub-contractors as though they are its own.

18.3 If, pursuant to Clause 15 (*Supply Chain Rights and Protections*), the Supplier proposes to sub-contract any of its responsibilities or obligations under this Agreement and subject to paragraph 29 of the Security Conditions, the Supplier shall:

(a) incorporate into the Sub-contract the terms of this Schedule 2.4 (*Security Management*) (with the exception of the Security Management Plan which shall be treated as described at Paragraph 18.3(b) below), including the obligations of this Paragraph 18 for any further sub-contracting, and such secrecy and security obligations as the Authority shall direct;

(b) incorporate into the Security Management Plan at Appendix B details of all Sub-contractor/ Supply chain security measures, together with any applicable security standards, contractual terms and policies of such Sub-contractor; and

(c) inform the Authority immediately if it becomes aware of any breach by the Sub-contractor of any secrecy or security obligation and, if requested to do so by the Authority, terminate the Sub-contract.

18.4 Where the Authority has consented to the placing of Sub-contracts, final copies of each Sub-contract shall, as soon as reasonably practicable, be sent by the Supplier to the Authority if requested under Clause 15.8 (*Appointment of Sub-contractors*) to do so. The Supplier shall be entitled to redact commercially sensitive or confidential pricing aspects of the Sub-contract(s) provided it does not undermine the security requirements of this Schedule 2.4 (*Security Management*).

19. SPECIAL SECURITY HANDLING REQUIREMENTS

19.1 In certain circumstances, the Authority may instruct the Supplier and the Supplier Personnel to comply with additional security requirements notified by the Authority to the Supplier from time to time. In such circumstances, the Supplier shall (and shall procure that the Supplier Personnel shall) comply with such instructions. Such instructions shall be included within the Supplier's Security Management Plan and when the wording of any necessary changes/ additions are Approved by the Authority, they will become contractual obligations. Where such additional security requirements impact the Supplier's price, ability to deliver the Services or existing obligations then the Supplier shall be entitled to address these impacts in accordance with the Change Control Procedure.

19.2 The Parties agree that a risk register setting out identified security risks and how responsibility for such risks are allocated as between the Parties (including any identified mitigations) will be maintained. Such risk register will be reviewed as part of the Security Working Group on a quarterly basis.

20. MALICIOUS SOFTWARE

20.1 The Supplier shall install and maintain Anti-Malicious Software or procure that Anti-Malicious Software is installed and maintained on any part of the systems, processes, and sites associated with provision of the Services which may Process Authority Data and ensure that such Anti-Malicious Software is configured to perform automatic software and definition updates as well as regular scans of the Information Management System and the Supplier System to check for, prevent the introduction of Malicious Software or where Malicious Software has been introduced into the

Information Management System and/or Supplier System, to identify, contain the spread of, and minimise the impact of Malicious Software.

20.2 If Malicious Software is found, the Parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Authority Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.

20.3 Any cost arising out of the actions of the Parties taken in compliance with the provisions of Paragraph 20.2 shall be borne by the Parties as follows:

(a) by the Supplier where the Malicious Software originates from:

(i) the Supplier Software;

(ii) the Third Party Software supplied by the Supplier; or

(iii) the Authority Data whilst the Authority Data is or was under the control of the Supplier,

unless, in the case of the Authority Data only, the Supplier can demonstrate that such Malicious Software was present in the Authority Data and not quarantined or otherwise identified by the Authority when the Authority provided the Authority Data to the Supplier; and

(b) by the Authority, in any other circumstance.

21. DATA PROCESSING, STORAGE, MANAGEMENT AND DESTRUCTION

21.1 In addition to the obligations on the Supplier set out Clause 19 (*Protection of Personal Data*) in respect of Processing Personal Data and compliance with the Data Protection Legislation, the Supplier shall:

(a) Process Authority Data only in the UK, except where the Authority has given its consent in writing to a transfer of the Authority Data to such other country;

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

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

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

(e) securely destroy all media that has held Authority Data at the end of life of that media in accordance with any specific requirements in this Agreement and, in the absence of any such requirements, as directed by the Authority.

22. EVENT LOGGING AND PROTECTIVE MONITORING

Protective Monitoring System

22.1 The Supplier must, and must ensure that Sub-contractors, implement an effective system of monitoring and reports (which shall be a commercial and production approved version which has passed relevant security procedures prior to production release and which is fully aligned to all updates released as part of a relevant

maintenance schedule), analysing access to and use of the Information Management System, the IT Environment and the Authority Data to:

(a) identify and prevent potential Security Breaches;

(b) respond effectively and in a timely manner to Security Breaches that do occur;

(c) identify and implement changes to the Information Management System and/or the Supplier System to prevent future Security Breaches; and

(d) help detect and prevent any potential criminal offence relating to fraud, bribery or corruption using the Information Management System and/or the IT Environment,

(collectively, the "**Protective Monitoring System**").

22.2 The Protective Monitoring System must provide for:

(a) event logs and audit records of access to the Supplier Information Management system and/or the Supplier System;

(b) regular reports and alerts to identify:

(i) changing access trends;

(ii) unusual usage patterns; or

(iii) the access of greater than usual volumes of Authority Data;

(c) the detection and prevention of any attack on the Information Management System and/or the IT Environment using common cyber-attack techniques; and

(d) any other matters required by the Security Management Plan.

Event logs

22.3 The Supplier must ensure that, unless the Authority otherwise agrees, any event logs do not log:

(a) Personal Data, other than identifiers relating to users; or

(b) sensitive data, such as credentials or security keys.

Provision of information to Authority

22.4 The Supplier must provide the Authority on request with:

(a) full details of the Protective Monitoring System it has implemented (which, in the case of SaaS Sub-contractors, will relate only to the tenancy environment or application relevant to the Services); and

(b) copies of monitoring logs and reports prepared as part of the Protective Monitoring System.

Changes to Protective Monitoring System

22.5 The Authority may at any time require the Supplier to update the Protective Monitoring System to:

(a) respond to a specific threat identified by the Authority;

(b) implement additional audit and monitoring requirements; and

(c) stream any specified event logs to the Authority's security information and event management system;

and in cases where the Authority's request under this Paragraph 22.5 amounts to a new requirement falling outside the scope of Clauses 16.5 and 16.7 (*Intellectual Property Rights, Authority Data and Security Requirements*) and Paragraph 7.1 of this Schedule 2.4 (*Security Management*), and subject to Paragraph 22.6 below, the Supplier shall be entitled to treat such request as a Contract Change under Schedule 8.2 (*Change Control Procedure*).

22.6 Where an aspect of the Services is provided via a Sub-contractor using software-as-a-service ("**SaaS Sub-contractor**"), the Supplier shall make reasonable endeavours to implement the changes described at Paragraph 22.5 above through the applicable contract change process agreed in the relevant Sub-contract with the SaaS Sub-contractor.

23. SECURITY WORKING GROUP

Role of the Security Working Group

23.1 The purpose of the Security Working Group is to provide a forum in which all IT security, information assurance and cyber security matters can be discussed, monitored and formulated in support of the secure delivery of the Services.

23.2 The Security Working Group shall:

(a) identify security risks and vulnerabilities and assess the potential impact on the Services of any perceived or changed security threats;

(b) review the security risk register described at Paragraph 19.2, escalating significant security risks as appropriate and in accordance with the escalation routes described in Schedule 8.1 (*Governance*) and discuss advice, guidance and information with respect to any identified security risks and issues;

(c) advise on the maintenance of Secure by Design status;

(d) provide advice on areas of risk analysis and management with respect to security matters impacting or having the potential to impact on the Services and record any residual security risks using the risk register described at Paragraph 19.2;

(e) providing advice on the implementation of Authority security policy, standards, requirements and any proposed solutions;

(f) providing advice to project staff on the security implications of any prosed changes to the configuration, operational requirements or protective marking level of Authority Data;

(g) reviewing and providing advice on security documentation;

(h) reviewing the Information Asset Register, identifying and advising on any changes as required;

(i) monitor compliance with the Security Management Plan, including the revision of any review and/or changes made in accordance with Paragraph 9.1;

(j) monitor developments in new technology, security controls and security risk management, encouraging innovation, transformation and the adoption of emerging changes in Good Industry Practice, the Security Policy Framework and the GSCP;

(k) discuss the impact or potential impact of any change or proposed change to the Supplier's or Sub-contractor's systems and processes, and the Services and/or associated processes; and

(l) such other actions as are required to fulfil the overarching objective of the Security Working Group as described at Paragraph 23.1 above.

23.3 The Security Working Group shall act at all times in accordance with the overarching principles and objectives of governance set out in Schedule 8.1 (*Governance*) including the Collaboration Requirements set out in Annex 8 of Schedule 8.1 (*Governance*).

Membership, attendance and frequency of meetings

23.4 Membership of the Security Working Group (**"SWH Members"**) shall be constituted as per the table set out in Appendix E to this Schedule 2.4 (*Security Management*).

23.5 The Security Working Group shall meet quarterly or more frequently where the Parties agree that it is reasonably necessary to do so, aligning to the frequency of meetings of the Boards set out in Schedule 8.1 (*Governance*) where it is appropriate to do so.

23.6 Each meeting of the Security Working Group shall be attended by the SWG Members, together with such other person as the Parties agree should attend appropriate to the subject matter being discussed at each individual meeting, and recognising any potential overlap of subject-matter being discussed at any relevant working group, Board or other governance body as described in Schedule 8.1 (*Governance*).

23.7 Each Party shall ensure that its SWG Members shall make all reasonable efforts to attend the respective meeting of the Security Working Group to which their attendance is required. If any SWG Member is not able to attend a meeting of the Security Working Group, that person shall use all reasonable endeavours to ensure that:

(a) a delegate attends the relevant meeting in their place who (wherever possible) is properly briefed, prepared and fully empowered to make all the decisions on the respective Party's behalf which may be required of that representative during that meeting; and

(b) that they are debriefed by such delegate after the relevant meeting.

23.8 If a Security Working Group meeting reasonably requires the attendance of particular persons at a meeting in compliance with Paragraph 23.6 above, the Parties must take reasonable action to ensure that those invitees attend the meeting.

23.9 The conduct of the business of each Security Working Group meeting shall be conducted as face-to-face meetings. Video conferencing or telephone conferencing may be substituted for face-to-face meetings where the Parties (acting reasonably) agree that it is reasonably practicable to do so considering the needs of both Parties' attendees.

23.10 The format of the agenda for each meeting and the minutes taken shall follow the approach set out in Annexes 4 and 5 of Schedule 8.1 (*Governance*).

APPENDIX A TO SCHEDULE 2.4

SECURITY ASPECTS LETTER

Ministry of Defence

REDACTED

Armed Forces Recruiting Programme

Ministry of Defence
REDACTED

Email: REDACTED

Cc to: REDACTED

For the Personal Attention Of:

REDACTED Serco CEO UK and Europe

Reference: 701577378 - AFRP

[Date][*insert contract signature date*]

CONTRACT NUMBER: 701577378 – AFRP

1. On behalf of the Secretary of State for Defence I hereby give you notice that all aspects of the work under the above Agreement are classified as OFFICIAL and the aspects defined below are specifically caveated as OFFICIAL-SENSITIVE:

OFFICIAL-SENSITIVE SECURITY ASPECTS
Sensitive Personal Data/images, as defined in the Data Protection Act 2018, not covered by Medical or Dental records, also marked with the Descriptor PERSONAL.
Any information stored or processed within the contracted infrastructure that pertains to the operational effectiveness or readiness of HM Armed Forces

Contract documentation that the Authority regards as OFFICIAL-SENSITIVE which, in accordance with GSCP, may include material whose compromise is likely to cause damage to the work or reputation of the Authority. The Authority reserves the right to increase the security level of contract documentation if it is deemed necessary, subject to the contractual change procedure. In this instance the documentation will be supplied over a secured email address or by the postal system.
Security assurance risk management information including (i) Lower Level Designs and other artefacts if they articulate the security posture; and (ii) Risk Management and assurance documents.
Aggregations of Personal Data, as defined in the Data Protection Act 2018.

2. If any security incidents occur related to this Agreement the details of the incident shall be reported in accordance with paragraphs 26-27 of the Security Conditions in Annex A of this document, as well as Paragraph 17 of this Schedule 2.4 (*Security Management*) and the incident management process set out in the Security Management Plan.

3. Information about this Agreement must not, without the approval of the Authority, be published or communicated to anyone except where necessary for the execution of this Agreement.

4. Your attention is drawn to the requirements of the "Security Conditions" and the provisions of the Official Secrets Act 1911-1989 in general, and specifically to the provisions of Section 2 of the Official Secrets Act 1911 (as amended by the Act of 1989) and the National Security Act 2023. In particular, you should take all reasonable steps to make sure that all individuals employed on any work in connection with this Agreement have notice of the above specified aspects and the aforementioned statutory provisions apply to them and will continue so to apply after the completion or earlier determination of this Agreement.

https://www.legislation.gov.uk/ukpga/1989/6/contents

5. Any access to classified information on MoD premises that may be needed will be in accordance with MoD security regulations under the direction of the MoD Project Security Officer (PSyO).

6. The attached Security Condition outlines the minimum measures required to safeguard OFFICIAL and OFFICIAL-SENSITIVE information and is provided to enable you to provide the required degree of protection.

7. The Parties agree that in executing this Agreement (including this Appendix A to Schedule 2.4 (*Security Management*)) you thereby confirm that the requirements of this Security Aspects Letter (SAL) and the Security Conditions (Annex A to this SAL) are understood and will be complied with.

Yours faithfully,

REDACTED

Annex A To
Security Aspects Letter
Dated [ ]

SECURITY CONDITIONS (for UK Contracts at OFFICIAL and OFFICIAL-SENSITIVE

1. The Supplier shall take all reasonable steps to adhere to the provisions specified in in this Annex A. The Supplier shall make sure that all individuals employed on any work in connection with this Agreement have notice that these provisions apply to them and shall continue so to apply after the completion or earlier termination of this Agreement.

Security Grading

2. All aspects associated with this Agreement are classified OFFICIAL. Some aspects are more sensitive and are classified as OFFICIAL-SENSITIVE. The Security Aspects Letter, issued by the Authority defines the OFFICIAL-SENSITIVE information that is furnished to the Supplier, or which is to be developed by it, under this Agreement. The Supplier shall mark all OFFICIAL-SENSITIVE documents which it originates or copies during this Agreement clearly with the OFFICIAL-SENSITIVE classification. However, the Supplier is not required to mark information/material related to this Agreement which is only OFFICIAL.

Official Secrets Acts

3. The Supplier's attention is drawn to the provisions of the Official Secrets Acts 1911-1989 in general, and to the provisions of Section 2 of the Official Secrets Act 1911 (as amended by the Act of 1989) in particular. The Supplier shall take all reasonable steps to make sure that all individuals employed on any work in connection with this Agreement (including Sub-contractors) have notice that these statutory provisions, or any others provided by the Authority, apply to them and shall continue so to apply after the completion or earlier termination of this Agreement.

Protection of OFFICIAL and OFFICIAL-SENSITIVE Information

4. The Supplier shall protect OFFICIAL and OFFICIAL-SENSITIVE information provided to it or generated by it in accordance with the requirements detailed in this Security Condition and any other conditions that may be specified by the Authority. The Supplier shall take all reasonable steps to prevent the loss or compromise of the information or from deliberate or opportunist attack.

5. Where the Supplier is required to store or process Authority classified information electronically, they shall comply with the requirements specified in ISNs, Defence Condition 658 and Defence Standard 05-138. Details can be found at the links below:

https://www.gov.uk/government/publications/industry-security-notices-isns

https://www.dstan.mod.uk/toolset/05/138/000004000.pdf

https://www.gov.uk/government/publications/defence-condition-658-cyber-flow-down

6. OFFICIAL and OFFICIAL-SENSITIVE information shall be protected in a manner to avoid unauthorised access. The Supplier shall take all reasonable steps to prevent the loss, compromise or inappropriate access of the information or from deliberate or opportunist attack.

7. All OFFICIAL and OFFICIAL-SENSITIVE material including documents, media and other material shall be physically secured to prevent unauthorised access. When not in use OFFICIAL and OFFICIAL- SENSITIVE documents/material shall be handled with care. As a minimum, when not in use, OFFICIAL-SENSITIVE material shall be stored under lock and key and in a lockable room, cabinets, drawers or safe and the keys/combinations are themselves to be subject to a level of physical security and control.

8. Disclosure of OFFICIAL and OFFICIAL-SENSITIVE information shall be strictly in accordance with the *"Need-to-know"* principle. Except with the written consent of the Authority, the Supplier shall not disclose any of the classified aspects of this Agreement detailed in the Security Aspects Letter other than to a person directly employed by the Supplier or Sub-contractor.

9. Any samples, patterns, specifications, plans, drawings or any other documents issued by or on behalf of the Authority for the purposes of this Agreement remain the property of the Authority and shall be returned on completion of this Agreement or, if directed by the Authority, destroyed in accordance with paragraph 32.

Access

10. Access to OFFICIAL and OFFICIAL-SENSITIVE information shall be confined to those individuals who have a *"Need-to-know"*, have been made aware of the requirement to protect the information and whose access is essential for the purpose of his or her duties.

11. The Supplier shall ensure that all individuals having access to OFFICIAL-SENSITIVE information have undergone basic recruitment checks. Suppliers shall apply the requirements of BPSS for all individuals having access to OFFICIAL-SENSITIVE information. Further details and the full requirements of the BPSS can be found at the GOV.UK website at:

https://www.gov.uk/government/publications/government-baseline-personnel-security-standard.

The following table lists the minimum System Role Clearances:

System Role Requirement	Clearance
Project supporting staff with no access to live system or data (e.g. facilities support	BPSS

System Role Requirement	Clearance
User access to system and controlled access to data (e.g. programme staff)	BPSS
Access, design, development and maintenance of MoD architecture and design documents	BPSS
Access to administrative functions without direct access to live data and no systems security log change access (e.g. SPOC agent)	SC
Access to Enterprise administrative functions, including access to live data or ability to change systems security logs (e.g. EA role)	SC

Hard Copy Distribution

12. OFFICIAL and OFFICIAL-SENSITIVE documents shall be distributed, both within and outside company premises in such a way as to make sure that no unauthorised person has access. It may be sent by ordinary post or commercial couriers in a single envelope. The words OFFICIAL or OFFICIAL-SENSITIVE shall not appear on the envelope. The envelope should bear a stamp or details that clearly indicates the full address of the office from which it was sent.

13. Advice on the distribution of OFFICIAL-SENSITIVE documents abroad or any other general advice including the distribution of OFFICIAL-SENSITIVE hardware shall be sought from the Authority.

Electronic Communication, Telephony and Facsimile Services

14. OFFICIAL information may be emailed unencrypted over the internet. OFFICIAL-SENSITIVE information shall normally only be transmitted over the internet encrypted using either a NCSC Commercial Product Assurance (CPA) cryptographic product or a MOD Approved cryptographic technique such as Transmission Layer Security (TLS). In the case of TLS both the sender and recipient organisations must be TLS enabled. Details of the required TLS implementation are available at:

https://www.ncsc.gov.uk/guidance/tls-external-facing-services

Details of the CPA scheme are available at:

https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa

Exceptionally, in urgent cases, OFFICIAL-SENSITIVE information may be emailed unencrypted over the internet where there is a strong business need to do so and only with the prior approval of the Authority.

15. OFFICIAL-SENSITIVE information shall only be sent when it is known that the recipient has been made aware of and can comply with the requirements of these Security Conditions and subject to any explicit limitations that the Authority shall require. Such limitations, including any regarding publication, further circulation or other handling instructions shall be clearly identified in the email sent with the material.

16. OFFICIAL information may be discussed with persons located both within the UK and overseas. OFFICIAL-SENSITIVE information may be discussed on fixed and mobile types of telephone within the UK, but not within earshot of unauthorised persons. However, OFFICIAL-SENSITIVE information should only be discussed where there is a strong business need to do so.

17. OFFICIAL information may be faxed to recipients located both within the UK and overseas, however OFFICIAL-SENSITIVE information may be faxed only to UK-based recipients.

Use of Information Systems

18. The detailed functions that must be provided by an IT system to satisfy the minimum requirements cannot all be described here; it is for the implementers to identify possible means of attack and ensure proportionate security mitigations are applied to prevent a successful attack.

19. The Supplier shall ensure 10 Steps to Cyber Security is applied in a proportionate manner for each IT and communications system storing, processing or generating MOD UK OFFICIAL or OFFICIAL-SENSITIVE information. 10 Steps to Cyber Security is available at:

https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

The Supplier shall ensure competent personnel apply 10 Steps to Cyber Security.

20. As a general rule, any communication path between an unauthorised user and the data can be used to carry out an attack on the system or be used to compromise or ex-filtrate data.

21. Within the framework of the 10 Steps to Cyber Security, the following describes the minimum security requirements for processing and accessing OFFICIAL-SENSITIVE information on IT systems.

a. Access. Physical access to all hardware elements of the IT system is to be strictly controlled. The principle of *"least privilege"* will be applied to any individual holding system administration rights . Users of the IT System: Administrators should not conduct *'standard'* User functions using their privileged accounts.

b. Identification and Authentication (ID&A). All systems shall have the following functionality:

- Up-to-date lists of authorised users.
- Positive identification of all users at the start of each processing session.

c. Passwords. Passwords are part of most Identification and Authorisation (ID&A) Security Measures. Passwords shall be 'strong' using an appropriate method to achieve this, for example including numeric and *"special"* characters (if permitted by the system) as well as alphabetic characters.

d. Internal Access Control. All systems shall have internal Access Controls to prevent unauthorised users from accessing or modifying the data.

e. Data Transmission. Unless the Authority authorises otherwise, OFFICIAL-SENSITIVE information shall be transmitted or accessed electronically (e.g. point to point computer links) via a public network like the Internet using a CPA product or equivalent as described in paragraph 14 above.

f. Security Accounting and Audit. Security relevant events fall into two (2) categories, namely legitimate events and violations. The following events shall always be recorded:

- All log on attempts whether successful or failed,
- Log off (including time out where applicable),
- The creation, deletion or alteration of access rights and privileges,
- The creation, deletion or alteration of passwords;

and, for each of the events listed above, the following information is to be recorded:

- Type of event,
- User ID (if known),
- Date & Time,
- Device ID (if known).

g. The accounting records shall have a facility to provide the System Manager with a hard copy of all or selected activity. There shall also be a facility for the records to be printed in an easily readable form. All security records are to be inaccessible to users without a need to know. If the operating system is unable to provide this then the equipment shall be protected by physical means when not in use i.e. locked away or the hard drive removed and locked away.

h. Integrity & Availability. The following supporting measures shall be implemented:

- Provide general protection against normally foreseeable accidents/mishaps and known recurrent problems (e.g. viruses, power supply variations),
- Defined Business Contingency Plan,
- Data backup with local storage,
- Anti-Malicious Software (implementation, with updates, of an acceptable industry standard Anti-virus software),
- Operating systems, applications and firmware should be supported,
- Patching of Operating Systems and Applications used shall be in line with the manufacturers recommended schedule. If patches cannot be applied an understanding of the resulting risk will be documented.

i. Logon Banners. Wherever possible, a *"Logon Banner"* shall be provided to summarise the requirements for access to a system which may be needed to institute legal action in case of any breach occurring. A suggested format for the text (depending on national legal requirements) could be:

"Unauthorised access to this computer system may constitute a criminal offence".

j. Unattended Terminals. Users are to be automatically logged off the system if their terminals have been inactive for some predetermined period of time, or systems must activate a password protected screen saver after thirty (30) minutes of inactivity, to prevent an attacker making use of an unattended terminal.

k. Internet Connections. Computer systems shall not be connected direct to the Internet or 'untrusted' systems unless protected by a firewall (a software based personal firewall is the minimum but risk assessment and management must be used to identify whether this is sufficient).

l. Disposal. Before IT storage media (e.g. disks) are disposed of, an erasure product shall be used to overwrite the data. This is a more thorough process than deletion of files, which does not remove the data.

Portable Electronic Devices

22. Portable Electronic Devices holding any MOD supplied or Supplier generated OFFICIAL-SENSITIVE information are to be encrypted using a CPA (or other MOD Approved) cryptographic product that is Approved by the Authority.

23. Unencrypted Portable Electronic Device and drives containing Personal Data are not to be taken outside of secure sites[1]. For the avoidance of doubt the term *"drives"* includes all removable, recordable media (e.g. memory sticks, compact flash, recordable optical media e.g. CDs and DVDs), floppy discs and external hard drives.

24. Any token, touch memory device or password(s) associated with the encryption package is to be kept separate from the machine whenever the machine is not in use, left unattended or in transit.

25. Portable Electronic Devices holding the Authorities' data are not to be left unattended in any public location. They are not to be left unattended in any motor vehicles either in view or in the boot or luggage compartment at any time. When the vehicle is being driven the Portable Electronic Device is to be secured out of sight in the glove compartment, boot or luggage compartment as appropriate to deter opportunist theft.

Loss and Incident Reporting

26. The Supplier shall immediately report any loss or otherwise compromise of any Defence Related Classified Material to the Authority. The term Defence Related Classified Material includes any information or asset that has been given a security classification by the UK MOD. The term also includes classified information and assets held by UK Defence

[1] Secure Sites are defined as either Government premises or a secured office on the Contractor premises.

suppliers which are owned by a third party e.g., NATO or another country for which the UK MOD is responsible.

27. In addition, any loss or otherwise compromise of Defence Related Classified Material is to be immediately reported to the UK MOD Defence Industry Warning, Advice and Reporting Point (WARP). This will assist the UK MOD in formulating a formal information security reporting process and the management of any associated risks, impact analysis and upward reporting to the UK MOD's Chief Information Officer (CIO) and, as appropriate, the Defence Supplier concerned. The UK MOD Defence Industry WARP will also advise the Defence Supplier what further action is required to be undertaken.

UK MOD Defence Industry WARP Contact Details
Email: DefenceWARP@mod.gov.uk (OFFICIAL with no NTK restrictions)
RLI Email: defencewarp@modnet.r.mil.uk (MULTIUSER)
Telephone (Office hours): +44 (0) 3001 583 640
Mail: Defence Industry WARP, DE&S PSyA Office
MOD Abbey Wood, NH2 Poplar-1 #2004, Bristol, BS34 8JH

28. Reporting instructions for any security incidents involving Defence Related Classified Material can be found in the Incident Reporting Industry Security Notice at:

https://www.gov.uk/government/publications/industry-security-notices-isns

Sub-Contracts

29. Except where Authority consent has been granted pursuant to paragraph 21.1(a) above, the Supplier may only Sub-contract elements of this Agreement to Sub-contractors within the United Kingdom seeking Authority approval as per Clause 15 (*Supply Chain Rights and Protections*). When sub-contracting to a Sub-contractor located in the UK the Supplier shall ensure that these Security Conditions shall be incorporated within the Sub-contract document. Notwithstanding the generality of the foregoing, the prior approval of the Authority shall be obtained should the Supplier wish to Sub-contract any OFFICIAL-SENSITIVE elements of this Agreement to a Sub-contractor located in another country. The first page of Appendix 5 (MOD Form 1686 (F1686)) of the Security Policy Framework Contractual Process chapter is to be used for seeking such approval. The MOD Form 1686 can be found at the Annex to:

https://assets.publishing.service.gov.uk/media/661f880e9bf3b7616bbd3d32/ISN_2024-05_Subcontracting_or_Collaborating_on_Classified_MOD_Programmes.pdfIf the Sub-contract is Approved, the Supplier shall incorporate these Security Conditions within the Sub-contract document.

Publicity Material

30. Suppliers wishing to release any publicity material or display hardware that arises from this Agreement shall seek the prior approval of the Authority. Publicity material includes open publication in the Supplier's publicity literature or website or through the media; displays at exhibitions in any country; lectures or symposia; scientific or technical papers, or any other occasion where members of the general public may have access to the information even if organised or sponsored by the Authority or any other government department.

Private Venture

31. Any defence related Private Venture derived from the activities of this Agreement are to be formally assessed by the Authority for determination of its appropriate classification. Suppliers are to submit a definitive product specification for PV Security Grading in accordance with the requirement detailed at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414857/20150310_PV_Ex_Guidance_Document.pdf

Promotions and Potential Export Sales

32. Suppliers wishing to promote, demonstrate, sell or export any material that may lead to the release of information or equipment classified OFFICIAL-SENSITIVE (including classified tactics, training or doctrine related to an OFFICIAL-SENSITIVE equipment) are to obtain the prior approval of the Authority utilising the MOD Form 680 process, as identified at:

https://www.gov.uk/mod-f680-applications

Destruction

33. As soon as no longer required, OFFICIAL and OFFICIAL-SENSITIVE information/material shall be destroyed in such a way as to make reconstitution unlikely, for example, by burning, shredding or tearing into small pieces. Advice shall be sought from the Authority when information/material cannot be destroyed or, unless already authorised by the Authority, when its retention is considered by the Supplier to be necessary or desirable. Unwanted OFFICIAL-SENSITIVE information/material which cannot be destroyed in such a way shall be returned to the Authority.

Interpretation/Guidance

34. Advice regarding the interpretation of the above requirements should be sought from the Authority.

35. Further requirements, advice and guidance for the protection of MOD information at the level of OFFICIAL-SENSITIVE may be found in Industry Security Notices at:

https://www.gov.uk/government/publications/industry-security-notices-isns

Audit

36. Where considered necessary by the Authority, the Supplier shall provide evidence of compliance with this Security Condition and/or permit the inspection of the Suppliers processes and facilities by representatives of the Authority to ensure compliance with these requirements unless, following best endeavours by the Supplier to facilitate such an inspection with respect to a relevant Sub-contractor, the Authority acting in its absolute discretion agrees that initiating such inspection is not practicable in the circumstances and agrees that alternative means of ensuring the relevant Sub-contractor's compliance with these requirements can be used.

Appendix B to Schedule 2.4

Security Management Plan

REDACTED

Security Management Plan: Appendices

REDACTED

Appendix C to Schedule 2.4

Cyber Risk Profile Security Requirements

HIGH CYBER RISK PROFILE REQUIREMENTS

Security Governance

L.01 Define and implement an information security policy, related processes and procedures.

L.02 Define and assign information security relevant roles and responsibilities.

L.03 Define and implement a policy which addresses information security risks within supplier relationships.

M.01 Define and implement a policy which provides for regular, formal information security related reporting.

M.02 Define and implement a repeatable risk assessment process.

Security culture and awareness

L.04 Define and implement a policy which ensures all functions have sufficient and appropriately qualified resources to manage the establishment, implementation and maintenance of information security.

L.05 Define employee (including contractor) responsibilities for information security.

L.06 Define and implement a policy to provide employees and contractors with information security training.

M.03 Define and implement a policy to detail specific employee and contractor responsibilities for information security before granting access to sensitive assets.

Information asset security

L.07 Define and implement a policy for ensuring sensitive information is clearly identified.

L.08 Define and implement a policy to control access to information and information processing facilities.

M.04 Define and implement a policy for storing, accessing, and handling sensitive information securely.

M.05 Define and implement a policy for data loss prevention.

M.06 Define, implement and test a policy for regular off-line back-up of data off-site.

M.07 Ensure the organisation has identified asset owners and asset owners control access to their assets.

Info-cyber systems security

L.09 Maintain annually renewed Cyber Essentials Plus Scheme

L.10 Define and implement a policy to control the exchanging of information via removable media.

L.11 Record and maintain the scope and configuration of the information technology estate.

L.12 Define and implement a policy to manage the access rights of user accounts.

L.13 Define and implement a policy to maintain the confidentiality of passwords.

M.08 Undertake administration access over secure protocols, using multi-factor authentication.

M.09 Define and implement a policy to assess vulnerabilities identified for which there are no countermeasures (e.g. a patch) available, undertake risk assessment and management.

M.10 Define and implement a policy to monitor network behaviour and review computer security event logs for indications of potential incidents.

M.11 Define and implement a policy to monitor user account usage and to manage changes of access rights.

M.12 Define and implement a policy to control remote access to networks and systems.

M.13 Define and implement a policy to control the use of authorised software.

M.14 Define and implement a policy to control the flow of information through network borders.

H.01 Maintain patching metrics and assess patching performance against policy.

H.02 Ensure wireless connections are authenticated.

H.03 Deploy network monitoring techniques which complement traditional signature-based detection.

H.04 Place application firewalls in front of critical servers to verify and validate the traffic going to the server.

H.05 Deploy network-based Intrusion Detection System (IDS) sensors on ingress and egress points within the network and update regularly with vendor signatures.

H.06 Define and implement a policy to control installations of and changes to software on any systems on the network.

H.07 Control the flow of traffic through network boundaries and police content by looking for attacks and evidence of compromised machines.

H.08 Design networks incorporating security countermeasures, such as segmentation or zoning.

H.09 Ensure Data Loss Prevention at egress points to inspect the contents of information and take appropriate action to prevent its inadvertent or malicious release.

Personnel security

L.14 Define and implement a policy for verifying an individual's credentials prior to employment.

L.15 Define and implement a process for employees and contractors to report violations of information security policies and procedures without fear of recrimination.

L.16 Define and implement a disciplinary process to take action against employees who violate information security policies or procedures.

M.13 Define and implement a policy for applying security vetting checks to employees.

M.14 Undertake personnel risk assessments for all employees and contractors and ensure those with specific responsibilities for information security have sufficient appropriate qualifications and appropriate levels of appropriate experience.

M.15 Define and implement a policy to secure organisational assets when individuals cease to be employed by your organisation.

Security Incident Management

L.17 Define and implement an incident management policy, which must include detection, resolution and recovery.

H.10 Proactively verify security controls are providing the intended level of security.

H.11 Define and implement a policy to ensure the continued availability of critical asset(s)/information during a crisis

MODERATE CYBER RISK PROFILE REQUIREMENTS

Security governance

L.01 Define and implement an information security policy, related processes and procedures.

L.02 Define and assign information security relevant roles and responsibilities.

L.03 Define and implement a policy which addresses information security risks within supplier relationships.

M.01 Define and implement a policy which provides for regular, formal information security related reporting.

M.02 Define and implement a repeatable risk assessment process.

Security culture and awareness

L.04 Define and implement a policy which ensures all functions have sufficient and appropriately qualified resources to manage the establishment, implementation and maintenance of information security.

L.05 Define employee (including contractor) responsibilities for information security.

L.06 Define and implement a policy to provide employees and contractors with information security training.

M.03 Define and implement a policy to detail specific employee and contractor responsibilities for information security before granting access to sensitive assets.

Information asset security

L.07 Define and implement a policy for ensuring sensitive information is clearly identified.

L.08 Define and implement a policy to control access to information and information processing facilities.

M.04 Define and implement a policy for storing, accessing, and handling sensitive information securely.

M.05 Define and implement a policy for data loss prevention.

M.06 Define, implement and test a policy for regular off-line back-up of data off-site.

M.07 Ensure the organisation has identified asset owners and asset owners control access to their assets.

Info-cyber systems security

L.09 Maintain annually renewed Cyber Essentials Plus Scheme.

L.10 Define and implement a policy to control the exchanging of information via removable media.

L.11 Record and maintain the scope and configuration of the information technology estate.

L.12 Define and implement a policy to manage the access rights of user accounts.

L.13 Define and implement a policy to maintain the confidentiality of passwords.

M.08 Undertake administration access over secure protocols, using multi-factor authentication.

M.09 Define and implement a policy to assess vulnerabilities identified for which there are no countermeasures (e.g. a patch) available, undertake risk assessment and management.

M.10 Define and implement a policy to monitor network behaviour and review computer security event logs for indications of potential incidents.

M.11 Define and implement a policy to monitor user account usage and to manage changes of access rights.

M.12 Define and implement a policy to control remote access to networks and systems.

M.13 Define and implement a policy to control the use of authorised software.

M.14 Define and implement a policy to control the flow of information through network borders.

Personnel security

L.14 Define and implement a policy for verifying an individual's credentials prior to employment.

L.15 Define and implement a process for employees and contractors to report violations of information security policies and procedures without fear of recrimination.

L.16 Define and implement a disciplinary process to take action against employees who violate information security policies or procedures.

M.13 Define and implement a policy for applying security vetting checks to employees.

M.15 Undertake personnel risk assessments for all employees and contractors and ensure those with specific responsibilities for information security have sufficient appropriate qualifications and appropriate levels of appropriate experience.

M.16 Define and implement a policy to secure organisational assets when individuals cease to be employed by your organisation.

Security incident management

L.17 Define and implement an incident management policy, which must include detection, resolution and recovery.

LOW CYBER RISK PROFILE REQUIREMENTS

Governance

L.01 Define and implement an information security policy, related processes and procedures.

L.02 Define and assign information security relevant roles and responsibilities.

L.03 Define and implement a policy which addresses information security risks within the supply chain.

Security culture and awareness

L.04 Define and implement a policy which ensures all functions have sufficient and appropriately qualified resources to manage the establishment, implementation and maintenance of information security.

L.05 Define employee (including contractor) responsibilities for information security.

L.06 Define and implement a policy to provide employees and contractors with information security training.

Information asset security

L.07 Define and implement a policy for ensuring sensitive information is clearly identified.

L.08 Define and implement a policy to control access to information and information processing facilities.

Info-cyber systems security

L.09 Maintain annually renewed Cyber Essentials Plus Scheme.

L.10 Define and implement a policy to control the exchanging of information via removable media.

L.11 Record and maintain the scope and configuration of the information technology estate.

L.12 Define and implement a policy to manage the access rights of user accounts.

L.13 Define and implement a policy to maintain the confidentiality of passwords.

Personnel security

L.14 Define and implement a policy for verifying an individual's credentials prior to employment.

L.15 Define and implement a process for employees and contractors to report violations of information security policies and procedures without fear of recrimination.

L.16 Define and implement a disciplinary process to take action against employees who violate information security policies or procedures.

Security Incident Management

L.17 Define and implement an incident management policy, which must include detection, resolution and recovery.

VERY LOW CYBER RISK PROFILE REQUIREMENTS

Info-Cyber Systems Security

VL.01 Maintain annually renewed Cyber Essentials Scheme.

Appendix D to Schedule 2.4

Security and Data Protection

REDACTED

Appendix E to Schedule 2.4

Security Working Group Membership

The Security Working Group shall comprise the membership listed in the Table below:

REDACTED