SCHEDULE 2.4

SECURITY REQUIREMENTS

1. DEFCON 658

1.1 The Supplier shall comply with the requirements of DEFCON 658 (Cyber) Ref: Edition 10/17, including each DEFCON referred to in DEFCON 658 [***Drafting Note**: comprising references to DEFCON 501, 530, 514 and 620*], in each case as amended or replaced from time to time:

20171016-DEFCON_658.pdf

1.2 This Schedule sets out the security requirements of the Authority to supplement DEFCON 658.

2. Order of precedence

2.1 If there is a conflict between this Schedule and DEFCON 658, the provisions of DEFCON 658 shall prevail over the provisions of this Schedule.

2.2 If there is a conflict between the provisions of this Schedule and any other provisions of this Agreement in relation to security requirements and management, this Schedule shall prevail to resolve such conflict.

2.3 If there is a conflict between the provisions of the Security Aspects Letter and the provisions of this Schedule, the Security Aspects Letter shall prevail to resolve such conflict.

3. Definitions

3.1 The definitions of DEFCON 658 (and each DEFCON referred to within it) shall apply to the extent any interpretation of DEFCON 658 (and/or each DEFCON referred to within it) is required in the context of this Schedule.

3.2 In addition, for the purposes of interpretation of this Schedule the following expressions shall have the following meanings:

Approve	means the Authority's prior written approval or consent, and "Approved" and "Approval" shall be construed accordingly;
Authority Data	means all data and information relating to the Authority, its business, affairs, operations, developments, facilities, accounts, clients, contacts, personnel, suppliers, finances, contractual arrangements, assets, programs, know-how, trade secrets and processes and any other data in relation to the Authority or used by it obtained by the Supplier through the performance of its obligations

	under this Agreement in whatever form that information may exist;
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 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;
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;
Supplier Personnel	means all persons employed by the Supplier to perform its obligations under this Agreement together with the Supplier's agents and contractors used in the performance of its obligations under this Agreement;
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 Level identified, will provide organisations with basic protection from the most prevalent forms of threat;
Cyber Risk Level	means the risk profile in line with Cyber Essentials criteria 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);

Good Industry Practice	means the exercise of skill, care and prudence which would at that time be reasonably expected from a leading supplier of services that are the same or substantially similar to the Services;
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;
Medium 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;
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;
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;
Security Management Plan	is the document produced and maintained in accordance with Paragraph 9 of this Schedule;
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.

3.3 In this Schedule, unless a contrary intention is expressly set out, all other capitalised terms shall have the same meaning as is set out in this Agreement (and/or the relevant DEFCON referred to).

4. Consequences of Breach

4.1 The Supplier shall (and shall ensure its Supplier Personnel and Sub-contractors) comply with the security requirements specified in this Schedule.

4.2 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.

4.3 Any breach of the security requirements specified in this Schedule may constitute a security breach and have implications for continued access to the Authority Sites and security clearance.

4.4 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.

4.5 A decision of the Authority on the question of whether the Supplier has taken or is taking reasonable steps as required by this Schedule shall be notified to the Supplier and shall be final and conclusive.

4.6 Any material breach of a provision of this Schedule (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.

5. Cyber Risk Profile

[*Note to bidders:* In accordance with DEFSTAN 05-138 (Defence Standard) issue 2 (2017), prior to the award of a contract, the following will occur:

a. First, a Risk Assessment (RA) is conducted to evaluate the degree of cyber risk to this contract based on the types of information involved, and will establish a Cyber Risk Level - Appendix C to this Schedule sets out the different Cyber Risk Levels for information;

b. Second, a Supplier Assurance Questionnaire (SAQ), is completed by suppliers who wish to be considered for a contract - this is done via Octavian tool - lead contractor in a consortium to respond on behalf of other members of the consortium;

c. Then, Authority will evaluate the SAQ results and any confirm if supporting evidence or actions required, such as a Cyber Implementation Plan (CIP), which will form a factor in considering if a contract should be awarded.

If a decision to award a contract is made, it may require supplemental security obligations / requirements to be included in this Schedule 2.4.

The drafting in DEFCON 658 accounts for a change in the Cyber Risk Level.]

5.1 In accordance with DEFCON 658, the Authority has determined the Cyber Risk Level appropriate to this Agreement and has notified the Supplier of that Cyber Risk Level, and shall notify the Supplier as soon as reasonably practicable where the Authority reassesses the Cyber Risk Level relating to this Agreement.

6. Certification Requirements

6.1 The Supplier shall be certified as compliant with:

(a) ISO/IEC 27001:2013 by a United Kingdom Accreditation Service-approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; 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.

6.2 The Supplier shall ensure that each Higher Risk Sub-contractor is certified as compliant with either:

(a) ISO/IEC 27001:2013 by a United Kingdom Accreditation Service-approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; 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.

6.3 The Supplier shall ensure that each Medium Risk Sub-contractor is certified compliant with Cyber Essentials.

6.4 The Supplier shall ensure that the Supplier and each Sub-contractor who is responsible for the secure destruction of Authority Data:

(a) securely destroys Authority Data only on Sites which are included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; and

(b) are certified as compliant with the NCSC Assured Service (CAS) Service Requirement Sanitisation Standard or an alternative standard as agreed by the Authority.

6.5 The Supplier shall provide the Authority with evidence of its and its Sub-contractor's compliance with the requirements set out in this Paragraph 6 before the Supplier or the relevant Sub-contractor (as applicable) may carry out the secure destruction of any Authority Data.

6.6 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 and, on request from the Authority, shall or shall procure that the relevant Sub-contractor shall:

(a) immediately ceases using the 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 6.

6.7 The Authority may agree to exempt, in whole or part, the Supplier or any Sub-contractor from the requirements of this Paragraph 6. Any exemption must be in writing to be effective. The Supplier must include the exemption in the Security Management Plan.

7. Security Lead

Appointment and role of Security Lead

7.1 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.

7.2 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.

7.3 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.

Training of Security Lead

7.4 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.

8. Compliance with the Security Policy Framework

8.1 The Supplier shall (and shall procure that its Supplier Personnel and Sub-contractors shall) at all times comply with the security requirements set out in the Security Policy Framework and provide a level of security which complies with the security measures and standards required by the Security Policy Framework and any Security Aspects Letter at Appendix A to this Schedule.

8.2 At the request of the Authority, the Supplier shall confirm to the Authority that the Supplier's security measures are consistent with this Schedule and the Security Policy Framework. Any inconsistency or non-compliance arising from a change to the Security Policy Framework or Security Aspects Letter shall be notified to the Authority and shall be addressed quarterly via the Security Working Group.

8.3 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.

8.4 The Supplier shall ensure that any and all information received from or held about the Authority, whether in respect of this Agreement or otherwise, is held in a secure fashion in accordance with HMG policy, 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.

9. Security Management Plan

9.1 The Supplier has developed a baseline Security Management Plan (as Approved by the Authority and set out in Appendix B of this Schedule) which it shall implement, operate and maintain (in accordance with continuous improvement principles) and which is subject to Approval by the Authority, and shall be in accordance with this Schedule and shall apply during the Term.

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

9.3 The Security Management Plan shall, unless otherwise specified by the Authority in this Schedule, 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.

9.4 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.

10. Amendment And Revision of the Security Management Plan

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

(a) emerging changes in Good Industry Practice and the Security Policy Framework;

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

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

(d) any reasonable request by the Authority.

10.2 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.

10.3 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.

10.4 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 shall not be implemented until Approved by the Authority.

11. OFFICIAL-SENSITIVE Information

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

11.2 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.

11.3 The Supplier shall include the requirements and obligations set out in Paragraph 11.2 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 11 to its Sub-contractors and through all levels of the supply chain to the lowest level where any OFFICIAL-SENSITIVE Information is handled.

12. Supplier Personnel

Vetting

12.1 All Supplier Personnel shall be vetted to the standards of BPSS (Baseline Personnel Security Standard).

12.2 All Supplier Personnel with administrator access to the systems shall have additional vetting applied to them to SC (Security Checks) standards. The personnel to which such Security Checks applies includes Database Administrators, Developers and System Architects.

12.3 All Supplier Personnel shall be vetted in accordance with Cabinet Office National Security standards MR 22 and 23 (to ensure staff are properly checked) and MR 48 (to ensure staff are properly trained).

Security Clearance

12.4 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.

12.5 Without prejudice to any other provision of this Agreement, where any member of Supplier Personnel or Sub-contractors has been involved in a material 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.

12.6 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.

12.7 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

12.8 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.

12.9 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.

12.10 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) or as advised to the Supplier by the Authority on an ongoing basis.

Conduct of Supplier Personnel

12.11 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 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.

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

12.13 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.

12.14 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.

12.15 Where there are reasonable concerns related to the security clearance and/or conduct of any 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

12.16 The Security Lead must inform and brief all relevant Supplier Personnel that they must notify him/her 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.

12.17 The Security Lead will notify the Authority of any such proposed visit to any country defined by the Authority.

12.18 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

12.19 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.

12.20 The Supplier shall bear the cost of any notice, instructions or decision of the Authority under this Paragraph 12 except where agreed pursuant to the Change Control Procedure.

13. Authority Sites

Access to the Authority Sites

13.1 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.

13.2 The Supplier and its 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.

13.3 The Supplier shall provide a list of the names and addresses of all 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.

13.4 The Supplier shall comply (and shall ensure its 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 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 to ensure they are in compliance with Authority rules, regulations, requirements and policies as these are made known to the Supplier by the Authority.

13.5 Only Supplier Personnel who have been appropriately security cleared and authorised by the Authority shall have access to the Authority Sites.

13.6 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 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 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

13.7 Supplier Personnel may be issued with a pass if so required which is expected to be permanent or time bound (not 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 a pass will indicate whether or not the holder is granted unescorted access to a given Authority site.

13.8 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.

13.9 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.

13.10 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.

13.11 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.

13.12 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

13.13 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.

13.14 The Authority reserves the right to permanently confiscate items covered under Paragraph 13.13 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

13.15 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.

13.16 Any Supplier equipment used on the Authority Sites that has at any stage been connected to the Authority's systems shall not be removed from the Authority Site unless agreed by the Authority.

13.17 Any equipment used at any time on the Supplier Site that contains the Authority's data shall be returned (through agreed channels) to the Authority at the end of this Agreement unless specifically told otherwise.

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

13.18 No Classified Matter (whether in written, photographic, diagrammatic or magnetic media form or any other form whatsoever) or equipment may be introduced or removed from an Authority Site without prior approval from the Authority.

Searches of bags, cases and packages carried by Supplier Personnel

13.19 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 13.13, 13.15, 13.16, or 13.18 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's Information Technology facilities by Supplier Personnel

13.20 Use of the Authority's IT facilities 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 IT facilities 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 IT facilities at all times.

13.21 The Supplier shall (and shall ensure that the Supplier Personnel shall) abide by the security operating procedures or policies of the Authority's IT facilities and data, and shall not attempt to gain unauthorised access to the Authority's IT facilities which are not essential for the provision of the work or services under this Agreement.

14. Authority Matter

14.1 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 is not a British citizen;

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

(c) 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;

(d) who is not a member of Supplier Personnel (save where anticipated pursuant to the Collaboration Agreement); and

(e) who is a member of Supplier Personnel but has no need to know the information for the proper performance of this Agreement.

14.2 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;

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

15. Electronic Access

15.1 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 additional rules for specific systems such as MODNet rules for MODNet access.

15.2 IT systems on which Authority Property, Authority Data and/or Classified Matter are held shall be accredited by the Authority's IT accreditor. The specific security and accreditation requirements will be determined by the Authority and agreed with the Supplier.

15.3 Electronic access to the IT systems on which the Authority Property/Authority Data/ Classified Matter is held shall only be allowed to authorised Supplier Personnel with the appropriate security clearance (as determined and Approved by the Authority).

16. Communications Security at Supplier Sites

16.1 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.

16.2 To assist in secure telephone and IT communications between the two 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.

16.3 If Paragraph 16.2 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.

17. Technical Access

17.1 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.

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

18. Security Breaches and Security Investigations

18.1 A security breach is an incident which 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.

18.2 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;

(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 breach of security.

18.3 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.

18.4 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.

18.5 Where unusual Security Events or Security Alerts are presented by the Supplier's programme team to the Supplier's corporate security manager, if deemed pertinent by the security manager, the Authority shall be notified and shall be notified of the security manager's recommendation. The existing obligations of reporting any Security Incidents shall remain as stated in DEFCON 658, and the parties shall comply with any requirements and timeframes imposed by the Authority's warning and reporting point (WARP) in relation to Security Incidents.

19. Sub-contracts

19.1 All references to Supplier Personnel and Supplier Sites in this Schedule 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.

19.2 Where the Supplier is List X accredited, any services relating to Classified Matter may only be sub-contracted to a List X accredited sub-contractor.

19.3 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.

19.4 If the Supplier proposes to sub-contract any of its responsibilities or obligations under this Agreement, the Supplier shall:

(a) submit for Approval of the Authority the name of the proposed sub-contractor, a statement of the work to be carried out, a copy of the proposed terms of the sub-contract and any other details known to the Supplier which the Authority reasonably requires;

(b) incorporate into the sub-contract the terms of this Schedule, including the obligations of this Paragraph 19 for any further sub-contracting, and such secrecy and security obligations as the Authority shall direct; and

(c) inform the Authority immediately 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.

19.5 Where the Authority has consented to the placing of sub-contracts, final copies of each sub-contract shall, at the request of the Authority, be sent by the Supplier to the Authority as soon as reasonably practicable. 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.

20. Special Security Handling Requirements

20.1 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 or existing obligations then the Supplier shall be entitled to address these impacts via change control.

The parties agree that the document entitled "TBD" as at the Effective Date contains a Risk Register setting out identified security risks and how responsibility for such risks are allocated as between the parties (including any identified mitigations). Such Risk Register will be reviewed as part of the Security Working Group on a quarterly basis.

APPENDIX A TO SCHEDULE 2.4

SECURITY ASPECTS LETTER

[ ]

[Redacted] Security Lead

1. **Information Systems and Services**

[REDACTED]

Telephone: [REDACTED]
Email: [ ] [REDACTED]

For the Personal Attention Of:

[ ]

[ ].

Reference: [Redacted]/[ ]

[Date]

CONTRACT NUMBER: [REDACTED]/[ ] – 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 contract are classified as OFFICIAL and the aspects defined below are specifically caveated as OFFICIAL-SENSITIVE for the purpose of DEFCON 660:

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. 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 accreditation risk management information including (i) Lower Level Designs and other artefacts if they articulate the security posture; and (ii) Risk Management and Accreditation Document Set Core 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 immediately reported after the incident is known in accordance with paragraphs 26-27 of the security conditions in Annex A of this document.

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

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). In particular, you should take all reasonable steps to make sure that all individuals employed on any work in connection with the contract 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 the contract.

[REDACTED]

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 Officer.

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. Will you please 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,

[ ]

Annex A To
Security Aspects Letter
Dated [ ]

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

Definitions

1. The term *"Authority"* for the purposes of the Annex means a Ministry of Defence (MOD) official acting on behalf of the Secretary of State for Defence.

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 the contract clearly with the OFFICIAL-SENSITIVE classification. However, the Supplier is not required to mark information/material related to the contract 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 the contract (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 the contract.

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. The Supplier shall apply Industry Security Notice (ISN) 2017/01 requirements to every industry owned IT and communication system used to store, process or generate MOD information including those systems containing OFFICIAL and/or OFFICIAL-SENSITIVE information. ISN 2017/01 details Defence Assurance and Risk Tool (DART) registration, IT security accreditation processes, risk assessment and risk management requirements. The ISN is available at:

[REDACTED]

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 the contract detailed in the Security Aspects Letter other than to a person directly employed by the Supplier or Sub-contractor, or [Service Provider].

9. Any samples, patterns, specifications, plans, drawings or any other documents issued by or on behalf of the Authority for the purposes of the contract remain the property of the Authority and shall be returned on completion of the contract 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 HMG Baseline Personnel Security Standard (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:

[REDACTED]

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
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:

[REDACTED]

Details of the CPA scheme are available at:

[REDACTED]

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 on fixed and mobile telephones 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.

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 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:

[REDACTED]

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 System Administrators. 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 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 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-Virus 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 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.

Laptops

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

23. Unencrypted laptops not on a secure site[1] are to be recalled and only used or stored in an appropriately secure location until further notice or until Approved full encryption is installed. Where the encryption policy cannot be met, a Risk Balance Case that fully explains why the policy cannot be complied with and the mitigation plan, which should explain any limitations on the use of the system, is to be submitted to the Authority for consideration. Unencrypted laptops and drives containing personal data are not to be taken outside of secure sites. 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 CIS devices 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 CIS 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 (after it is known) any loss or other compromise of any OFFICIAL or OFFICIAL-SENSITIVE information to the Authority.

27. Any security incident involving any MOD owned, processed, or Supplier generated OFFICIAL or OFFICIAL-SENSITIVE information defined in the contract Security Aspects Letter shall be immediately reported (after it is known) to the MOD Defence Industry Warning, Advice and Reporting Point (WARP), within the Joint Security Co-ordination Centre (JSyCC). This will assist the JSyCC in formulating a formal information security reporting process and the management of any associated risks, impact analysis and upward reporting to the MOD's Chief Information Officer (CIO) and, as appropriate, the company concerned. The MOD WARP will also advise the Supplier what further action is required to be undertaken. Accordingly, in accordance with Industry Security Notice 2014/02 as may be subsequently updated at:

[REDACTED]

JSyCC WARP Contact Details

Email: For those with access to the RLI: CIO-DSAS-JSyCCOperations

Email: For those without access to the RLI: CIO-DSAS-[REDACTED]

Telephone: [REDACTED]

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

Working Hours: [REDACTED]

Out of Hours/Duty Officer Phone: [REDACTED]

Fax: [REDACTED]

Mail: Joint Security Co-ordination Centre (JSyCC), [REDACTED]

Sub-Contracts

28. The Supplier may Sub-contract any elements of this Agreement to Sub-contractors within the United Kingdom notifying the Authority. 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. The prior approval of the Authority shall be obtained should the Supplier wish to Sub-contract any OFFICIAL-SENSITIVE elements of the contract to a Sub-contractor located in another country. The first page of Appendix 5 (MOD Form [REDACTED] ([REDACTED])) of the Security Policy Framework Contractual Process chapter is to be used for seeking such approval. The MOD Form [REDACTED]
can be found at Appendix 5 at:

[REDACTED]

If the Sub-contract is Approved, the Supplier shall incorporate these security conditions within the Sub-contract document.

Publicity Material

29. 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 MOD, Services or any other government department.

Private Venture

30. 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:

[REDACTED]

Promotions and Potential Export Sales

31. 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 [REDACTED] process, as identified at:

[REDACTED]

Destruction

32. 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

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

34. 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:

[REDACTED]

Audit

35. 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.

Appendix B to Schedule 2.4

Baseline Security Management Plan

[*To be inserted here*]

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 Scheme Plus Certification.

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 Scheme Plus Certification.

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 Scheme Plus Certification.

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 certification.