## SCHEDULE 8

## Security and Information Management

### 1. Definitions

1.1 In this Schedule the definitions set out in Schedule 1 (Definitions) shall apply.

### 2. Introduction

2.1 This Schedule sets out:

(a) the arrangements the Contractor must implement before, and comply with when, providing the Services and performing its other obligations under this Contract to ensure the security of the Authority Data and the Contractor System;

(b) the Certification Requirements applicable to the Contractor and each of those SubContractors which handles and/or processes Authority Data;

(c) the tests which the Contractor shall conduct on the Contractor System during the contract duration;

(d) the Contractor's obligations to return or destroy Authority Data on the expiry or earlier termination of this Contract; and

(e) the process to be followed in the event of a Breach of Security.

### 3. Principles of Security

3.1 The Contractor acknowledges that the Authority places great emphasis on the confidentiality, integrity and availability of the Authority Data.

3.2 Notwithstanding the involvement of the Authority in assessing the arrangements which the Contractor implements to ensure the security of the Authority Data and the Contractor System, the Contractor shall be, and shall remain, responsible for:

(a) the security, confidentiality, integrity and availability of the Authority Data whilst that Authority Data is under the control of the Contractor or any of its Sub-Contractors; and

(b) the security of the Contractor System.

3.3 The Contractor shall:

(a) comply with the security requirements in as set out in the Security Aspects Letter at Annex B to this Schedule;

(b) ensure that each Sub-Contractor that Processes Authority Data complies with the Sub-Contractor Security Requirements at Annex C to this Schedule;

(c) provide the name of the Contractor's security officer to the Authority;

(d) ensure the Contractor's security officer liaises with the Authority’s security officer in relation to any security matters at Government Establishments; and

(e) ensure that all Contractor Personnel (including Sub-Contractors, Agents and Representatives) have the required UKAS Security Clearances required to enable them to carry out their duties in providing the Services as set out in the Security Aspects Letter.

**4. Information Security Approval Statement**

4.1 The Contractor's Transition Plan and Service Delivery Plan sets out how the Contractor shall ensure compliance with the requirements of this Schedule 8 (Security and Information Management), including the requirements imposed on Sub-Contractors by Annex C, from Effective Date.

4.2 The Contractor may not use the Contractor System to Process Authority Data unless and until:

(a) the Contractor has procured the conduct of an IT Health Check of the Contractor System by a CHECK Service Provider or a CREST Service Provider in accordance with paragraph 7.1; and

(b) the Authority has issued the Contractor with an Information Security Approval Statement in accordance with the process set out in this paragraph 4.

4.3 The Authority may require, and the Contractor shall provide the Authority and its authorised representatives with:

(a) access to the Contractor Personnel;

(b) access to the Contractor System to audit the Contractor and its Sub-Contractors' compliance with this Contract; and

(c) such other information and/or documentation that the Authority or its authorised representatives may reasonably require,

to assist the Authority to establish whether the arrangements which the Contractor and its SubContractors have implemented to ensure the security of the Authority Data and the Contractor System are consistent with the representations in the Transition Plan and the Service Delivery Plan. The Contractor shall provide the access required by the Authority in accordance with this paragraph within twenty (20) Business Days of receipt of such request, except in the case of a Breach of Security in which case the Contractor shall provide the Authority with the access that it requires within 24 hours of receipt of such request.

**5. Compliance**

5.1 The Contractor shall regularly review and update the Security and Information Management Plan, and provide such to the Authority, at least once each Contract Year pursuant to Clause 30.5 (Change) of the Contract.

5.2 The Contractor shall notify the Authority within ten (10) Business Days after becoming aware of:

(a) a significant change to the components or architecture of the Contractor System;

(b) a new risk to the components or architecture of the Contractor System;

(c) a change in the risk profile;

(d) a significant change to any risk component;

(e) a significant change in the quantity of Personal Data held within the Service;

(f) a proposal to change any of the Sites from which any part of the Services are provided; and/or

(g) an ISO27001 and/or IASME Gold audit report produced in connection with the Certification Requirements indicates significant concerns,

and such notice shall include a summary of any Changes the Contractor reasonably believes are required as a result of (a) to (g) (as applicable) above. If the Authority considers that a Change is required then it shall proceed in accordance with the Change Control Procedure.

5.3 The Contractor shall, upon written request by the Authority, provide the Authority with evidence of its and its Sub-Contractor's compliance with the requirements set out in this Schedule 8 (Security and Information Management).

**6. Certification Requirements**

6.1 The Contractor and all relevant Sub-Contractors shall be certified as compliant with:

(a) ISO/IEC 27001:2013 and/or IASME Gold 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/or IASME Gold; and

(b) Cyber Essentials PLUS,

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

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

(a) ISO/IEC 27001:2013 and/or IASME Gold 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/or IASME Gold; 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 Contractor shall ensure that each Medium Risk Sub-Contractor is certified compliant with Cyber Essentials.

6.4 The Contractor shall ensure that they 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/or IASME Gold; 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 Contractor shall notify the Authority as soon as reasonably practicable and, in any event within ten (10) Business Days, if the Contractor 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 cease 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. **7. Security Testing**

7.1 The Contractor shall, at its own cost and expense procure and conduct:

(a) testing of the Contractor System by a CHECK Service Provider or a CREST Service Provider ("**IT Health Check**"); and

(b) such other security tests as may be required by the Authority,

the IT Health Check shall be repeated not less than once every twelve (12) months during the Contract Term and the results of each such test submitted to the Authority for review in accordance with this paragraph.

7.2 In relation to each IT Health Check, the Contractor shall:

(a) agree with the Authority the aim and scope of the IT Health Check;

(b) promptly, and no later than ten (10) Business Days, following the receipt of each IT Health Check report, provide the Authority with a copy of the full report;

(c) in the event that the IT Health Check report identifies any vulnerabilities, the Contractor shall:

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

(A) how the vulnerability will be remedied;

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

(1) within three months of the date the Contractor received the IT Health Check report in the case of any vulnerability categorised with a severity of “medium”;

(2) within one month of the date the Contractor received the IT Health Check report in the case of any vulnerability categorised with a severity of “high”; and

(3) within five (5) Business Days (or such other time period as agreed in writing between the Parties) of the date the Contractor received the IT Health Check report in the case of any vulnerability categorised with a severity of “critical”;

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

(ii) comply with the Vulnerability Correction Plan; and

(iii) conduct such further tests on the Service as are required by the Vulnerability Correction Plan to confirm that the Vulnerability Correction Plan has been complied with.

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

7.4 If any testing conducted by or on behalf of the Contractor identifies a new risk, new threat, vulnerability or exploitation technique that has the potential to affect the security of the Contractor System, the Contractor shall within five (5) Business Days (or such other time period as agreed in writing between the Parties) of becoming aware of such risk, threat, vulnerability or exploitation technique provide the Authority with a copy of the test report and:

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

(b) where and to the extent applicable, remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in

order to reduce the attack surface of the Contractor System) within the timescales set out in the test report or such other timescales as may be agreed with the Authority.

7.5 The Contractor shall conduct such further tests of the Contractor System as may be required by the Authority from time to time to demonstrate compliance with its obligations set out this Schedule and the Contract.

**8. Monitoring and Reporting**

8.1 The Contractor shall:

(a) ensure that the Joint Risk Register reflects any security risks identified in relation to the operation of the Services and the handling of Authority Data and is kept up to date; and

(b) report Breaches of Security in accordance with the approved Incident Management Process and paragraph 10.3 below.

**9. Malicious Software**

9.1 The Contractor shall install and maintain Anti-Malicious Software or procure that Anti-Malicious Software is installed and maintained on any part of the Contractor System 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 to check for, prevent the introduction of Malicious Software or where Malicious Software has been introduced into the Contractor System, to identify, contain the spread of, and minimise the impact of Malicious Software.

9.2 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.

9.3 Any cost arising out of the actions of the parties taken in compliance with the provisions of paragraph 9.2 shall be borne by the parties as follows:

(a) by the Contractor where the Malicious Software originates from the Contractor Software, the Third Party Software supplied by the Contractor or the Authority Data (whilst the Authority Data was under the control of the Contractor) unless the Contractor can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Authority when provided to the Contractor; and

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

**10. Breach of Security**

10.1 The Contractor shall monitor security risk impacting upon the operation of the Service.

10.2 If either Party becomes aware of a Breach of Security, it shall notify the other in accordance with the Incident Management Process.

10.3 The Contractor shall, upon it becoming aware of a Breach of Security or attempted Breach of Security, immediately take all reasonable steps necessary to invoke its Incident Management Process which shall:

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

(b) remedy such Breach of Security to the extent possible;

(c) apply a tested mitigation against any such Breach of Security; and

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

10.4 Following the Breach of Security or attempted Breach of Security, the Contractor shall as soon as reasonably practicable and, in any event, within five (5) Business Days (or such other time period as agreed in writing between the Parties), provide to the Authority full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Authority.

10.5 In the event that any action is taken in response to a Breach of Security or attempted Breach of Security as a result of non-compliance by the Contractor, its Sub-Contractors and/or all or any part of the Contractor System with this Contract, then such remedial action shall be completed at no additional cost to the Authority.

## ANNEX A

## BASELINE SECURITY REQUIREMENTS

### 1 Security Classification of Information

1.1 If the provision of the Services requires the Contractor to Process Authority Data which is classified as:

(a) OFFICIAL-SENSITIVE, the Contractor shall implement such additional measures as agreed with the Authority from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards; and/or

(b) SECRET or TOP SECRET, the Contractor shall only do so where it has notified the Authority prior to receipt of such Authority Data and the Contractor shall implement additional measures as agreed with the Authority from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards.

### 2 End User Devices

1.1 The Contractor must manage, and must ensure that all Sub-Contractors manage, all end-user devices used by the Contractor on which Authority Data is Processed in accordance the following requirements:

1.1.1 the operating system and any applications that Process or have access to Authority Data must be in current support by the vendor, or the relevant community in the case of open source operating systems or applications;

1.1.2 users must authenticate before gaining access;

1.1.3 all Authority Data must be encrypted using an encryption tool agreed to by the Authority;

1.1.4 the end-user device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the end-user device is inactive;

1.1.5 the end-user device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Authority Data;

1.1.6 the Contractor or Sub-Contractor, as applicable, can, without physical access to the end-user device, remove or make inaccessible all Authority Data on the device and prevent any user or group of users from accessing the device;

1.1.7 all end-user devices are within in the scope of any current Cyber Essentials Plus certificate held by the Contractor, or any ISO/IEC 27001 (at least ISO/IEC 27001:2013) and/or IASME Gold certification issued by a UKAS-approved certification body, where the scope of that certification includes the Services.

1.2 The Contractor must comply, and ensure that all Sub-Contractors comply, with the recommendations in NCSC Device Guidance, as updated, amended or replaced from time to time, as if those recommendations were incorporated as specific obligations under this Contract.

1.3 Where there is any conflict between the requirements of this Schedule 8 (Security and Information Management) and the requirements of the NCSC Device Guidance, the requirements of this Schedule will take precedence.

**2 Encryption**

2.1 The Contractor must ensure, and must ensure that all Sub-Contractors ensure, that Authority Data is encrypted:

2.1.1 when stored at any time when no operation is being performed on it; and

2.1.2 when transmitted.

2.2 Where the Contractor, or a Sub-Contractor, cannot encrypt Authority Data the Contractor must:

2.2.1 immediately inform the Authority of the subset or subsets of Authority Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;

2.2.2 provide details of the protective measures the Contractor or Sub-Contractor (as applicable) proposes to take to provide equivalent protection to the Authority as encryption; and

2.2.3 provide the Authority with such information relating to the Authority Data concerned, the reasons why that Authority Data cannot be encrypted and the proposed protective measures as the Authority may require.

2.3 The Authority, the Contractor and, where the Authority requires, any relevant Sub-Contractor shall meet to agree appropriate protective measures for the unencrypted Authority Data.

2.4 Where the Authority and Contractor reach agreement, the Contractor must update the Security and Information Management Plan to include:

2.4.1 the subset or subsets of Authority Data not encrypted and the circumstances in which that will occur; and

2.4.2 the protective measure that the Contractor and/or Sub-Contractor will put in place in respect of the unencrypted Authority Data.

2.1 Where the Authority and Contractor do not reach agreement within forty (40) Business Days of the date on which the Contractor first notified the Authority that it could not encrypt certain Authority Data, either Party may refer the matter to be determined in accordance with Schedule 30 (Dispute Resolution Procedure).

**3 Personnel Security**

3.1 All Contractor Personnel shall be subject to a pre-employment check before they may participate in the provision and or management of the Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; verification of the individual's criminal record.

3.2 The Authority and the Contractor shall review the roles and responsibilities of the Contractor Personnel in order to enable the Authority to determine which roles require additional vetting and a specific national security vetting clearance (e.g. a Counter Terrorist Check). Roles which are likely to require additional vetting and a specific national security vetting clearance include system administrators whose role would provide those individuals with privileged access to IT systems which Process Authority Data or data which, if it were Authority Data, would be classified as OFFICIAL-SENSITIVE.

3.3 The Contractor shall not permit Contractor Staff who fail the security checks required by paragraphs 3.1 and 3.2 to be involved in the management and/or provision of the Services except where the Authority has expressly agreed in writing to the involvement of the named individual in the management and/or provision of the Services.

3.4 The Contractor shall ensure that Contractor Staff are only granted such access to Authority Data as is necessary to enable the Contractor Staff to perform their role and to fulfil their responsibilities.

3.5 The Contractor shall ensure that Contractor Staff who no longer require access to the Authority Data (e.g. they cease to be employed by the Contractor or any of its Sub-Contractors), have their rights to access the Authority Data revoked within one (1) Business Day.

3.6 The Contractor shall ensure that Contractor Staff that have access to the Sites, the Shared Data Environment or the Authority Data receive regular training on security awareness that reflects the degree of access those individuals have to the Sites, the Shared Data Environment or the Authority Data.

3.7 The Contractor shall ensure that the training provided to Contractor Staff under paragraph 3.6 includes training on the identification and reporting fraudulent communications intended to induce individuals to disclose Personal Data or any other information that could be used, including in combination with other Personal Data or information, or with other techniques, to facilitate unauthorised access to the Sites, the Shared Data Environment or the Authority Data ("phishing").

**4 Identity, Authentication and Access Control**

4.1 The Contractor shall operate an access control regime to ensure:

(a) all users and administrators of the Contractor System are uniquely identified and authenticated when accessing or administering the Services; and

(b) all persons who access the Sites are identified and authenticated before they are allowed access to the Sites.

4.2 The Contractor shall apply the 'principle of least privilege' when allowing persons access to the Contractor System and Sites so that such persons are allowed access only to those parts of the Sites and the Contractor System they require.

4.3 The Contractor shall retain records of access to the Sites and to the Contractor System and shall make such record available to the Authority on request.

**5 Audit and Protective Monitoring**

5.1 The Contractor shall collect audit records which relate to security events in Contractor System or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Contractor audit records should (as a minimum) include regular reports and alerts setting out details of access by users of the Contractor System, to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of Authority Data.

5.2 In addition to any requirement in Clause 40 (Cyber), the Contractor shall:

(a) implement audit and monitoring of the Contractor System sufficient to comply with any applicable Relevant Requirements and to prevent or detect any Prohibited Act;

(b) keep sufficient records to demonstrate compliance with the requirements of paragraph 5.2(a) to the Authority; and

(c) make those records and any documents describing the audit and monitoring undertaken to the Authority on request.

5.3 The Contractor and the Authority shall work together to establish any additional audit and monitoring requirements for the Contractor System.

5.4 The retention periods for audit records and event logs must be agreed with the Authority and documented in the Security and Information Management Plan.

## 6 Secure Architecture

6.1 The Contractor shall design the Contractor System in accordance with:

(a) the NCSC "Security Design Principles for Digital Services", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/security-design-principles-digitalservices-main;

(b) the NCSC "Bulk Data Principles", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main; and

(c) the NSCS "Cloud Security Principles", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles and which are summarised below:

(i) "Cloud Security Principle 1: data in transit protection" which, amongst other matters, requires that user data transiting networks should be adequately protected against tampering and eavesdropping;

(ii) "Cloud Security Principle 2: asset protection and resilience" which, amongst other matters, requires that user data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure;

(iii) "Cloud Security Principle 3: separation between users" which, amongst other matters, requires that a malicious or compromised user of the service should not be able to affect the service or data of another;

(iv) "Cloud Security Principle 4: governance framework" which, amongst other matters, requires that the Contractor should have a security governance framework which coordinates and directs its management of the Services and information within it;

(v) "Cloud Security Principle 5: operational security" which, amongst other matters, requires that the Services need to be operated and managed securely in order to impede, detect or prevent a Breach of Security;

(vi) "Cloud Security Principle 6: personnel security" which, amongst other matters, requires that where Contractor Staff have access to Authority Data and/or the Authority System that those personnel be subject to appropriate security screening and regular security training;

(vii) "Cloud Security Principle 7: secure development" which, amongst other matters, requires that the Services be designed and developed to identify and mitigate threats to their security;

(viii) "Cloud Security Principle 8: supply chain security" which, amongst other matters, requires the Contractor to ensure that appropriate security controls are in place with its Sub-Contractors and other Contractors;

(ix) "Cloud Security Principle 9: secure user management" which, amongst other matters, requires the Contractor to make the tools available for the Authority to securely manage the Authority's use of the Service;

(x) "Cloud Security Principle 10: identity and authentication" which, amongst other matters, requires the Contractor to implement appropriate controls in order to ensure that access to Service interfaces is constrained to authenticated and authorised individuals;

(xi) "Cloud Security Principle 11: external interface protection" which, amongst other matters, requires that all external or less trusted interfaces with the Services should be identified and appropriately defended;

(xii) "Cloud Security Principle 12: secure service administration" which, amongst other matters, requires that any IT system which is used for administration of a cloud service will have highly privileged access to that service;

(xiii) "Cloud Security Principle 13: audit information for users" which, amongst other matters, requires the Contractor to be able to provide the Authority with the audit records it needs to monitor access to the Service and the Authority Data held by the Contractor and/or its Sub-Contractors;

(xiv) "Cloud Security Principle 14: secure use of the service" which, amongst other matters, requires the Contractor to educate Contractor Staff on the safe and secure use of the Contractor System.

**ANNEX B**

**SECURITY ASPECTS LETTER**

**Defence Marine Services**
Rm 221, 24 Store, Bldg

1/117

HM Naval Base Portsmouth

Hampshire

Serco Limited
Serco House
Hook
Hampshire
RG27 9UY

**Reference:** DMS-NG SAL

**Date:**

Our Reference: 073247450

PO1 3LT

---

**Dear Sir / Madam,**

**DEFENCE MARITIME SERVICES NEXT GENERATION ITN**
**CONTRACT 1 - SUPPORT TO IN-PORT MARINE SERVICES AND DELIVERY OF A VESSEL REPLACMENT**
**CONTRACT NO: 073247450**

**SECURITY ASPECTS LETTER**

1 On behalf of the Secretary of State for Defence, I hereby give the Tenderer notice of the information or assets connected with, or arising from, the referenced Invitation to Negotiate (ITN) that constitute classified material.

2 Aspects that constitute OFFICIAL-SENSITIVE for the purposes of DEFCON 660 are specified below. These aspects must be fully safeguarded. The Security Condition at Appendix 1 (UK Official and UK OfficialSensitive Contractual Security Conditions) to this Annex E outlines the minimum measures required to safeguard OFFICIAL-SENSITIVE assets and information.

| ASPECT | CLASSIFICATION |
|---|---|
| The existence of the DMS NG Programme | OFFICIAL |
| Value of the DMS NG Programme to UK Operational Capability | OFFICIAL |
| The DMS NG Master Data Assumptions List (MDAL) | OFFICIAL SENSITIVE |
| The Project, Statement of Technical Requirement | OFFICIAL SENSITIVE |
| All artefacts released into the DSP Data Room in support of Project ITN, provided for the purpose of instructing informed bids | OFFICIAL SENSITIVE |
| Daily Movements Signal & Changes (Portsmouth and Devonport) | OFFICIAL |
| KHM Clyde Movements Signal | OFFICIAL |
| KHM Harbour Operations Signal | OFFICIAL |
| 2 Weekly Movements Plan | OFFICIAL - SENSITIVE |
| Monthly Movements Plan | OFFICIAL - SENSITIVE |
| FOST 4 Weekly Look Ahead | OFFICIAL - SENSITIVE |
| Faslane Security Standing Orders | OFFICIAL - SENSITIVE |
| HMNB Clyde Contractor & Visitor Security Policy Document | OFFICIAL - SENSITIVE |
| HMNB Clyde Accreditation Policy | OFFICIAL - SENSITIVE |
| HMNB Clyde Accreditation Procedures | OFFICIAL - SENSITIVE |

| | |
|---|---|
| HMNB Clyde Portable Electronic Device Policy | OFFICIAL - SENSITIVE |
| BRd 8754 - Submarine Towed Array Systems Recovery and Deployment | OFFICIAL - SENSITIVE |
| BRd 9424 (2) - Fleet Operating Orders (FLOOS) (Volume 2), Chapter 4. | OFFICIAL - SENSITIVE |
| Port Operational Management Safety Report (POMSR) | OFFICIAL - SENSITIVE |

3 The Tenderer's attention is drawn to the provisions of the Official Secrets Act (OSA) 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 the Tenderer should take all reasonable steps to make sure that all individuals employed on any work in connection with this ITN have notice of the above specified aspects and that the aforementioned statutory provisions apply to them and will continue to apply should the ITN be unsuccesful.

4 Will the Tenderer please confirm that:

4.1 this definition of the classified aspects of the referenced ITN has been brought to the attention of the person directly responsible for security of classified material;

4.2 the definition is fully understood;

4.3 measures can, and will, be taken to safeguard the classified aspects identified herein in accordance with applicable national laws and regulations. The requirement and obligations set out above and in any contractual document can and will be met and that the classified information shall be protected in accordance with applicable national laws and regulations; and

4.4 all employees of the company who will have access to classified information have either signed the OSA Declaration Form in duplicate and one (1) copy is retained by the Company Security Officer or have otherwise been informed that the provisions of the OSA apply to all classified information and assets associated with this ITN.

5 Clyde Naval Base security policy states that access requests for Foreign/Dual National Contractors or Naturalised British Citizens (born outside the UK) must only be made in exceptional circumstances where they are for highly specialised engineering techniques utilising SQEP that is unavailable in the UK. Only suitably cleared UK Nationals will be permitted to work in or visit Clyde Naval Base.

6 If the Tenderer has any difficulty either in interpreting this definition of the classified aspects or in safeguarding them, will the Tenderer please let me know immediately.

7 Classified Information associated with this ITN must not be published or communicated to anyone without the approval of the MOD Contracting Authority.

8 Any access to classified information or assets on MOD premises that may be needed will be subject to MOD security regulations under the direction of the MOD Project Officer in accordance with DEFCON 76 – attached at Appendix 2 (Contractor's Personnel at Government Establishments) of this Annex E. Yours faithfully,

DMS-NG Contract Lead

Copy via email to:
ISAC-Group (MULTIUSER)
COO-DSR-IIPCSy (MULTIUSER)
UKStratComDD-CyDR-CySAAS-021

# APPENDIX 1 - UK OFFICIAL AND UK OFFICIAL-SENSITIVE CONTRACTUAL SECURITY CONDITIONS

**Contract no: 798934450 In-Port Marine Services and Delivery of a Vessel Replacement Programme**

**21 Dec 22**

**Purpose**

1 This document provides guidance for Contractors where classified material provided to or generated by the Contractor is graded UK OFFICIAL or UK OFFICIAL-SENSITIVE. Where the measures requested below cannot be achieved or are not fully understood, further advice should be sought from the UK Designated Security Authority (Email: COO-DSRIIPCSy@mod.gov.uk).

**Definitions**

2 The term "**Authority**" for the purposes of this Annex means the HMG Contracting Authority.

3 The term "**Classified Material**" for the purposes of this Annex means classified information and assets.

**Security Grading**

4 The SENSITIVE caveat is used to denote UK OFFICIAL material that is of a particular sensitivity and where there is a need to reinforce the 'need to know'. The Security Aspects Letter, issued by the Authority shall define the UK OFFICIAL-SENSITIVE material that is provided to the Contractor, or which is to be developed by it, under this Contract. The Contractor shall mark all UK OFFICIAL and UK OFFICIAL-SENSITIVE documents which it originates or copies during the Contract with the applicable security grading.

**Security Conditions**

5 The Contractor shall take all reasonable steps to adhere to the provisions specified in the Contract or listed in this Annex E. The Contractor shall make sure that all individuals employed on any work in connection with the Contract have notice that these provisions apply to them and shall continue to apply after the completion or earlier termination of the Contract. In accordance with Part D (Records) of Schedule 6 (Governance, Management Information, Reports, Records and Audit) the Authority must state the data retention periods to allow the Contractor to produce a data management policy. If Tenderers are a Contractor located in the UK their attention is also drawn to the provisions of the Official Secrets Acts 1911 to 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.

**Protection of UK OFFICIAL and UK OFFICIAL-SENSITIVE Classified Material**

6 The Contractor shall protect UK OFFICIAL and UK OFFICIAL-SENSITIVE material provided to 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 Contractor shall take all reasonable steps to prevent the loss or compromise of classified material whether accidentally or from deliberate or opportunist attack.

7 Once the Contract has been awarded, where Contractors are required to store or process UK MOD classified information electronically, they are required to register the IT system onto the Defence Assurance Risk Tool (DART). Details on the registration process can be found in the 'Industry Security Notices (ISN)' on Gov.UK website. ISNs 2017/01, 04 and 06, Defence Condition 658 and Defence Standard 05-138 details the DART registration, IT security accreditation processes, risk assessment/management and Cyber security requirements which can be found in the following links:

https://www.gov.uk/government/publications/industry-security-notices-isns.
http://dstan.gateway.isg-r.r.mil.uk/standards/defstans/05/138/000002000.pdf
https://www.gov.uk/government/publications/defence-condition-658-cyber-flow-down

8 All UK classified material including documents, media and other assets must be physically secured to prevent unauthorised access. When not in use UK OFFICIAL and UK OFFICIALSENSITIVE material shall be handled with care to prevent loss or inappropriate access. As a minimum UK OFFICIAL-SENSITIVE material shall be stored under lock and key and shall be placed in a lockable room, cabinets, drawers or safe and the keys/combinations shall be subject to a level of control.

9 Disclosure of UK OFFICIAL and UK OFFICIAL-SENSITIVE material must be strictly controlled in accordance with the "need to know" principle. Except with the written consent of the Authority, the Contractor shall not disclose the Contract or any provision thereof to any person other than to a person directly employed by the Contractor or Sub-Contractor.

10 Except with the consent in writing of the Authority the Contractor shall not make use of the Contract or any information issued or provided by or on behalf of the Authority otherwise than for the purpose of the Contract, and, same as provided for in paragraph 8 above, the Contractor shall not make use of any article or part thereof similar to the articles for any other purpose.

11 Subject to any intellectual property rights of third parties, nothing in this Security Condition shall restrict the Contractor from using any specifications, plans, drawings and other documents generated outside of this Contract.

12 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 must be returned on completion of the Contract or, if directed by the Authority, destroyed in accordance with paragraph 35.

**Access**

13 Access to UK OFFICIAL and UK OFFICIAL-SENSITIVE material 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 their duties.

14 The Contractor shall ensure that all individuals requiring access to UK OFFICIAL-SENSITIVE information have undergone basic recruitment checks. This should include establishing proof

of identity; confirming that they satisfy all legal requirements for employment by the Contractor; and verification of their employment record. Criminal record checks should also be undertaken where permissible under national/local laws and regulations. This is in keeping with the core principles set out in the UK Government (HMG) Baseline Personnel Security Standard (BPSS) which can be found at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/714002/HMG_Baseline_Personnel_Security_Standard_-_May_2018.pdf

**Hard Copy Distribution**

15 UK OFFICIAL and UK OFFICIAL-SENSITIVE documents may be distributed, both within and outside Contractor premises in such a way as to make sure that no unauthorised person has access. It may be sent by ordinary post in a single envelope. The words UK OFFICIAL or UK OFFICIAL-SENSITIVE must not appear on the envelope. The envelope must bear a stamp or marking that clearly indicates the full address of the office from which it was sent. Commercial Couriers may be used.

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

**Electronic Communication and Telephony and Facsimile Services**

17 UK OFFICIAL information may be emailed unencrypted over the internet. UK OFFICIALSENSITIVE information shall normally only be transmitted over the internet encrypted using either a National Cyber Security Centre (NCSC) Commercial Product Assurance (CPA) cryptographic product or a UK MOD approved cryptographic technique such as Transmission Layer Security (TLS). In the case of TLS both the sender and recipient organisations must have 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

18 Exceptionally, in urgent cases UK OFFICIAL-SENSITIVE information may be emailed unencrypted over the internet where there is a strong business need to do so, but only with the prior approval of the Authority. However, it 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 require. Such limitations including any regarding publication, further circulation or other handling instructions shall be clearly identified in the email sent with the material.

19 UK OFFICIAL information may be discussed on fixed and mobile telephones with persons located both within the country of the Contractor and overseas. UK OFFICIAL-SENSITIVE information may be discussed on fixed and mobile telephones only where there is a strong business need to do so and only with the prior approval of the Authority.

20 UK OFFICIAL information may be faxed to recipients located both within the country of the Contractor and overseas, however UK OFFICIAL-SENSITIVE information may be transmitted only where there is a strong business case to do so and only with the prior approval of the Authority.

**Use of Information Systems**

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

22 The Contractor should ensure 10 steps to Cyber Security (link below) is applied in a proportionate manner for each IT and communications system storing, processing or generating UK OFFICIAL or UK OFFICIAL-SENSITIVE information. The Contractor should ensure competent personnel apply 10 steps to Cyber Security.

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

23 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.

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

24.1 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.

24.2 Identification and Authentication (ID&A). All systems are to have the following functionality:

a) up-to-date lists of authorised users; and

b) positive identification of all users at the start of each processing session.

24.3 Passwords. Passwords are part of most ID&A security measures. Passwords are to be "strong" using an appropriate method to achieve this, e.g. including numeric and "special" characters (if permitted by the system) as well as alphabetic characters.

24.4 Internal Access Control. All systems are to have Internal Access Controls to prevent unauthorised users from accessing or modifying the data.

24.5 Data Transmission. Unless the Authority authorises otherwise, UK OFFICIAL-SENSITIVE information may only 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 16 (Hard Copy Distribution) above.

24.6 Security Accounting and Audit. Security relevant events fall into two categories, namely legitimate events and violations.

a) The following events shall always be recorded:

i all log on attempts whether

successful or failed; ii log off (including

time out where applicable); iii the

creation, deletion or alteration of access

rights and privileges; and iv the

creation, deletion or alteration of

passwords.

b) For each of the events listed above, the following information is to be recorded:

i type of event; ii user ID; iii

date & time; and iv device

ID.

The accounting records are to have a facility to provide the System Administrator with a hard copy of all or selected activity. There also must 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 must be protected by physical means when not in use i.e. locked away or the hard drive removed and locked away.

24.7 Integrity & Availability. The following supporting measures are to be implemented:

a) provide general protection against normally foreseeable accidents/mishaps and known recurrent problems (e.g. viruses and power supply variations);

b) defined Business Contingency Plan;

c) data backup with local storage;

d) anti-virus software (implementation, with updates, of an acceptable industry standard

anti-virus software);

e) operating systems, applications and firmware should be supported; and

f) patching of operating systems and applications used are to be in line with the manufacturers recommended schedule. If patches cannot be applied an understanding of the resulting risk will be documented.

24.8 Logon Banners. Wherever possible, a "Logon Banner" will 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"*

24.9 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 15 minutes of inactivity, to prevent an attacker making use of an unattended terminal.

24.10 Internet Connections. Computer systems must 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).

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

**Laptops**

25 Laptops holding any UK OFFICIAL-SENSITIVE information shall be encrypted using a CPA product or equivalent as described in paragraph 17 (Electronic Communication and Telephony and Facsimile Services) above.

26 Unencrypted laptops 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 (CDs and DVDs), floppy discs and external hard drives.

27 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.

28 Portable CIS 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 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**

29 The Contractor shall immediately report any loss or otherwise compromise of any OFFICIAL or OFFICIAL-SENSITIVE material to the Authority. In addition any loss or other compromise of any UK MOD owned, processed or UK MOD Contractor generated UK OFFICIAL or UK OFFICIAL-SENSITIVE material is to be immediately reported to the UK MOD Defence Industry Warning, Advice and Reporting Point (WARP). This will assist the 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

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

appropriate, the Contractor concerned. The UK MOD WARP will also advise the Contractor what further action is required to be undertaken.

**WARP Contact Details**

**Email:** DefenceWARP@mod.gov.uk (OFFICIAL with no NTK restrictions)
**RLI Email:** defencewarp@modnet.rli.uk (MULTIUSER)
**Telephone (Office hours):** +44 (0) 30 6770 2185
**Mail:** Defence Industry WARP, DE&S PSyA Office
MOD Abbey Wood, NH2 Poplar-1 #2004, Bristol, BS34 8JH

30 Reporting instructions for any security incidents involving MOD classified material can be found in Industry Security Notice 2017/03 as may be subsequently updated at:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/651683/ISN_2017-03_-_Reporting_of_Security_Incidents.pdf

**Sub-Contracts**

31 Where the Contractor wishes to sub-contract any elements of a Contract to Sub-Contractors within its own country or to Contractors located in the UK such sub-contracts will be notified to the contracting Authority. The Contractor shall ensure that these Security Conditions are incorporated within the sub-contract document.

32 The prior approval of the Authority shall be obtained should the Contractor wish to sub-contract any UK OFFICIAL-SENSITIVE elements of the Contract to a Sub-Contractor facility located in another (third party) country. The first page of Appendix 5 (MOD Form 1686 (F1686) of the GovS 007 Security Contractual Process chapter is to be used for seeking such approval. The MOD Form 1686 can be found at Appendix 5 at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/710891/2018_May_Contractual_process.pdf

33 If the sub-contract is approved, the Contractor will flow down the Security Conditions in line with paragraph 31 (Sub-Contracts) above to the Sub-Contractor. Contractors located overseas may seek further advice and/or assistance from the Authority with regards the completion of F1686.

**Publicity Material**

34 Contractors wishing to release any publicity material or display assets that arise from a Contract to which these Security Conditions apply must seek the prior approval of the Authority. Publicity material includes open publication in the Contractor'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 UK Government.

**Physical Destruction**

35 As soon as no longer required, UK OFFICIAL and UK OFFICIAL-SENSITIVE material shall be destroyed in such a way as to make reconstitution very difficult or impossible, 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 Contractor to be necessary or desirable. Unwanted UK

OFFICIAL-SENSITIVE information/material which cannot be destroyed in such a way shall be returned to the Authority.

**Interpretation/Guidance**

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

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

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

**Audit**

38 Where considered necessary by the Authority the Contractor shall provide evidence of compliance with this Security Condition and/or permit the inspection of the Contractors processes and facilities by representatives of the Contractors' National/Designated Security Authorities or the Authority to ensure compliance with these requirements.

## APPENDIX 2 - DEFCON 76: CONTRACTOR'S PERSONNEL AT GOVERNMENT ESTABLISHMENTS

**Contract no:**
**798934450 In-Port Marine Services and Delivery of a Vessel Replacement Programme**

**21 Dec 22**

**Contractor's Representatives**

1 The Contractor shall submit in writing to the Authority for approval, initially and as necessary from time to time, a list of those of its Representatives who may need to enter a Government Establishment for the purpose of, or in connection with, work under the Contract, giving such particulars as the Authority may require, including full details of birthplace and parentage of any such Representative who:

1.1 was not born in the United Kingdom; or

1.2 if they were born in the United Kingdom, was born of parents either or both of whom were not born in the United Kingdom.

2 The Authority shall issue passes for those Representatives who are approved by it in accordance with paragraph 1 herein for admission to a Government Establishment and a

Representative shall not be admitted unless in possession of such a pass. Passes shall remain the property of the Authority and shall be surrendered on demand or on completion of the work.

3 Notwithstanding the provisions of paragraphs 1 and 2 hereof if, in the opinion of the Authority, any Representative of the Contractor shall misconduct themselves, or it shall not be in the public interest for any person to be employed or engaged by the Contractor, the Contractor shall remove such person without delay on being required to do so and shall cause the work to be performed by such other person as may be necessary.

4 The decision of the Authority upon any matter arising under paragraphs 1 to 3 inclusive shall be final and conclusive.

**Observance of Regulations**

5 The following provisions apply:

5.1 The Contractor shall ensure that his Representatives have the necessary probity (by undertaking the Government's Baseline Personnel Security Standard) and, where applicable,

are cleared to the appropriate level of security when employed within the boundaries of a Government Establishment.

5.2 Where the Contractor requires information on the Government's Baseline Personnel Security Standard (the Standard) or security clearance for his Representatives or is not in possession of the relevant rules, regulations or requires guidance on them, he shall apply in the first instance to the Project Manager/Equipment Support Manager.

5.3 On request, the Contractor shall be able to demonstrate to the Authority that the Contractor's processes to assure compliance with the standard have been carried out satisfactorily. Where that assurance is not already in place, the Contractor shall permit the Authority to inspect the processes being applied by the Contractor to comply with the Standard.

5.4 The Contractor shall comply and shall ensure that his Representatives comply with the rules, regulations and requirements that are in force whilst at that Establishment which shall be provided by the Authority on request.

5.5 When on board ship, compliance with the rules, regulations, and requirements shall be in accordance with the Ship's Regulations as interpreted by the Officer in Charge. Details of those rules, regulations and requirements shall be provided on request by the Officer in Charge.

**ANNEX C**

**1. Application of Annex**

1.1 This Annex applies to all Sub-Contractors that Process Authority Data.

1.2 The Contractor must:

(a) ensure that those Sub-Contractors comply with the provisions of this Annex;
(b) keep sufficient records to demonstrate that compliance to the Authority; and
(c) ensure that its Transition Plan includes Deliverable Items, Milestones and Milestone Dates that relate to the design, implementation and management of any systems used by Sub-Contractors to Process Authority Data.

**2. Designing and managing secure solutions**

2.1 The Sub-Contractor shall implement their solution(s) to mitigate the security risks in accordance with the NCSC's Cyber Security Design Principles https://www.ncsc.gov.uk/collection/cybersecurity-design-principles.

2.2 The Sub-Contractor must assess their systems against the NCSC Cloud Security Principles: https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloudsecurity/implementing-the-cloud-security-principles at their own cost and expense to demonstrate that the people, process, technical and physical controls have been delivered in an effective way. The Sub-Contractor must document that assessment and make that documentation available to the Authority on the Authority's request.

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

3.1 The Sub-Contractor must not Process any Authority Data outside the UK. The Authority may permit the Sub-Contractor to Process Authority Data outside the UK and may impose conditions on that permission, with which the Sub-Contractor must comply. Any permission must be in writing to be effective.

3.2 The Sub-Contractor must when requested to do so by the Authority:

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

(b) satisfy the Authority that their data destruction/deletion practices comply with UK GDPR requirements and follows all relevant NCSC guidance; and
(c) maintain an asset register of all Authority supplied information, data and equipment to ensure Authority assets are returned and/or deleted.

**4. Personnel Security**

4.1 The Sub-Contractor must perform appropriate checks on their staff before they may participate in the provision and or management of the Services. Those checks must include all preemployment checks required by the HMG Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; verification of the individual's employment history; and verification of the individual's criminal record. The HMG Baseline Personnel Security Standard is at https://www.gov.uk/government/publications/government-baseline-personnel-securitystandard.

4.2 The Sub-Contractor must, if the Authority requires, at any time, ensure that one or more of the Sub-Contractor's staff obtains security check clearance in order to Process Authority Data containing Personal Data above certain volumes specified by the Authority, or containing Special Category Personal Data.

4.3 Any Sub-Contractor staff who will, when performing the Services, have access to a person under the age of 18 years must undergo Disclosure and Barring Service checks.

**5. End User Devices**

5.1 The Contractor must manage, and must ensure that all Sub-Contractors manage, all end-user devices used by the Contractor on which Authority Data is Processed in accordance the following requirements:

(a) the operating system and any applications that Process or have access to Authority Data must be in current support by the vendor, or the relevant community in the case of open source operating systems or applications;
(b) users must authenticate before gaining access;
(c) all Authority Data must be encrypted using an encryption tool agreed to by the Authority;
(d) the end-user device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the end-user device is inactive;
(e) the end-user device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Authority Data;
(f) the Contractor or Sub-Contractor, as applicable, can, without physical access to the end-user device, remove or make inaccessible all Authority Data on the device and prevent any user or group of users from accessing the device; and
(g) all end-user devices are within in the scope of any current Cyber Essentials Plus certificate held by the Contractor, or any ISO/IEC 27001 (at least ISO/IEC 27001:2013) and/or IASME Gold certification issued by a UKAS-approved certification body, where the scope of that certification includes the Services.

5.2 The Contractor must comply, and ensure that all Sub-Contractors comply, with the recommendations in NCSC Device Guidance, as updated, amended or replaced from time to time, as if those recommendations were incorporated as specific obligations under this Contract.

5.3 Where there is any conflict between the requirements of this Schedule 8 (Security and Information Management) and the requirements of the NCSC Device Guidance, the requirements of this Schedule will take precedence.

**6. Encryption**

6.1 The Contractor must ensure, and must ensure that all Sub-Contractors ensure, that Authority Data is encrypted:

(a) when stored at any time when no operation is being performed on it; and (b) when transmitted.

6.2 Where the Contractor, or a Sub-Contractor, cannot encrypt Authority Data the Contractor must:

(a) immediately inform the Authority of the subset or subsets of Authority Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;

(b) provide details of the protective measures the Contractor or Sub-Contractor (as applicable) proposes to take to provide equivalent protection to the Authority as encryption; and

(c) provide the Authority with such information relating to the Authority Data concerned, the reasons why that Authority Data cannot be encrypted and the proposed protective measures as the Authority may require.

6.3 The Authority, the Contractor and, where the Authority requires, any relevant Sub-Contractor shall meet to agree appropriate protective measures for the unencrypted Authority Data.

6.4 Where the Authority and Contractor reach agreement, the Contractor must update the Security and Information Management Plan to include:

(a) the subset or subsets of Authority Data not encrypted and the circumstances in which that will occur; and

(b) the protective measure that the Contractor and/or Sub-Contractor will put in place in respect of the unencrypted Authority Data.

6.5 Where the Authority and Contractor do not reach agreement within forty (40) Business Days of the date on which the Contractor first notified the Authority that it could not encrypt certain Authority Data, either Party may refer the matter to be determined in accordance with Schedule 30 (Dispute Resolution Procedure).

**7. Patching and Vulnerability Scanning**

7.1 The Sub-Contractor must proactively monitor Contractor vulnerability websites and ensure all necessary patches and upgrades are applied to maintain security, integrity and availability in accordance with the NCSC Cloud Security Principles.

**8. Third Party Sub-Contractors**

8.1 The Sub-Contractor must not transmit or disseminate the Authority Data to any other person unless specifically authorised by the Authority. Such authorisation must be in writing to be effective and may be subject to conditions.

8.2 The Sub-Contractor must not, when performing any part of the Services, use any software to Process the Authority Data where the licence terms of that software purport to grant the licensor rights to Progress the Authority Data greater than those rights strictly necessary for the use of the software.