1 Standard Security Requirements

Unless otherwise set out in these requirements, all defined terms shall have the meaning ascribed to them in the applicable Purchaser's terms and conditions.

For the purpose of these requirements, references to "Purchaser Information" shall mean any and all data, information or material provided by the Purchaser to the Supplier under the Agreement, including without limitation: (a) Background IPR; (b) Confidential Information; (c) Controlled Material; (d) Foreground IPR; (e) Personal Data and (f) and any information or data created by the Supplier based on any of the foregoing.

Whilst the Supplier use, stores or accesses any Purchaser Information, it shall comply with the requirements below, unless otherwise agreed in writing.

1.1 Cyber Essentials Scheme

The Supplier shall hold, and continue to hold, a valid Cyber Essentials Certificate prior to contracting with the Purchaser. Details of the Cyber Essentials Scheme can be found here:

https://www.gov.uk/government/publications/cyber-essentials-scheme-overview;

1.2 Access Management

1.2.1 The Supplier shall ensure that access to Purchaser Information is restricted to only those of its employees, consultants, contractors, professional advisors and approved sub-contractor(s) ("**Permitted Parties**") who have a need to know the information.

1.2.2 Where the Supplier allows Permitted Parties to use personal devices to access Purchaser Information in carrying out their duties, the Supplier shall implement an appropriate acceptable use policy and appropriate security controls commensurate with the sensitivity of the Purchaser Information.

1.3 **Password Management**

The Supplier shall ensure that:

1.3.1 Passwords used to access electronic devices, information systems and/or IT networks that hold, store, process or are otherwise used to access Purchaser Information:

(a) are unique and require use of alphabetic, numeric and special characters;

(b) follow the password requirements set out in Cyber Essentials for General User account;

(c) contain a minimum of 15 characters for privileged accounts (e.g. local administrators);

(d) contain a minimum of 20 characters for highly privileged account passwords (e.g. domain administrators); and

(e) are not written down nor shared.

1.3.2 The Supplier shall ensure automatic logoff or locking is implemented and enforced, requiring all users to re-input their password to regain access if they have been inactive for a pre-determined period of time, which, as a minimum, should be no longer than 20 minutes of inactivity.

1.4 **Data Backup**

Where the Supplier holds Purchaser Information in an electronic format, the Supplier shall ensure all Purchaser Information is backed up in a separate location, at least 1km away from the primary location, with which has physical access and commensurate information security controls in place.

1.5 **Portable Devices**

1.5.1 The Supplier shall ensure that all portable devices including, without limitation, laptops, tablets, smartphones, removable media or any other devices that hold or have access to any Purchaser Information, use an industry standard full disk encryption solution.

1.5.2 The Supplier shall extend patch management under the Cyber Essentials Scheme to all portable devices which hold or have access to Purchaser Information.

1.6 **Incident Reporting, Response & Recovery**

1.6.1 For the purpose of these requirements, an '**Information Security Incident'** shall mean the actual or suspected occurrence of:

(a) any unauthorised access to, or use or disclosure of, any Purchaser Information; and/or

(b) any unauthorised or accidental destruction, damage, deletion and/or loss of any Purchaser Information (including copies).

1.6.2 The Supplier shall notify the Purchaser in accordance with paragraph 1.6.6 and without undue delay (and in any event within twenty-four (24) hours) of becoming aware of, or reasonably suspecting, an Information Security Incident. The Supplier shall provide the Purchaser with details of the Information Security Incident as are reasonably required by the Purchaser including, without limitation and to the extent then known:

(a) the categories, volume and description of the Purchaser Information affected by the Information Security Incident and, where applicable, the categories and numbers of Data Subjects whose Personal Data is affected;

(b) the name and contact details of the Supplier's data protection officer or other relevant contact from whom more information may be obtained;

(c) a description of the likely impact on the Purchaser Information affected by the Information Security Incident; and

(d) a description of the measures taken, or proposed to be taken, to address the Information Security Incident.

1.6.3 The Supplier acknowledges that the Purchaser may be required to the provide information relating to the Information Security Incident to third parties (including its customers or any regulatory bodies) and the Supplier hereby consents to such disclosure provided that the Purchaser shall ensure any recipient treats such information as being confidential to the Supplier.

1.6.4 Upon becoming aware of, or reasonably suspecting, an Information Security Incident, the Supplier shall promptly take all reasonable steps necessary to remedy the event, mitigate the impact and prevent its reoccurrence, and shall notify the Purchaser of the remedial steps taken. The Supplier shall co-operate with the Purchaser and take such reasonable steps as are directed by the Purchaser to assist in the investigation, mitigation and remediation of each Information Security Incident.

1.6.5 In the event of an Information Security Incident, the Supplier shall not inform any third party without first obtaining the Purchaser's prior written consent, unless notification is required by applicable law that applies to the Supplier, in which case the Supplier shall to the extent permitted by such law inform the Purchaser of that legal requirement, provide a copy of the proposed notification and consider any comments made by the Purchaser before notifying any third party of the Information Security Incident.

1.6.6 The Supplier shall:

(a) notify its point of contact at BAE Systems; and

(b) email the IT Security Operations Mailbox: itsecurityoperations@baesystems.com

1.7 Training and Vetting

The Supplier shall ensure that all Permitted Parties are appropriately security vetted and trained on a continual basis. Training shall cover, as a minimum, the following areas: identifying security breaches, information security risks, and the legal obligations associated with Purchaser Information that is stored, handled and processed by such Permitted Parties.

1.8 Physical Access

The Supplier shall implement appropriate and effective physical security measures at its premises in accordance with Good Industry Practice, including establishing a policy which requires Permitted Parties to securely store Purchaser Information they have access to in the course of discharging their duties and adequately dispose of any printed documents in a secure manner e.g. by putting them through a cross cut shredder and disposing of them securely.

1.9 Decommissioning & Disposal

1.9.1 On termination or expiry of the contract with the Purchaser, the Supplier shall cease use of all Purchaser Information and, at the Purchaser's absolute discretion, either: (i) promptly (and in any event within 28 (twenty eight) calendar days of expiry or termination) permanently delete all Purchaser Information in its possession so that it cannot be recovered or reconstructed or (ii) require the Supplier to return a complete copy of all Purchaser Information to the Purchaser by secure file transfer in a format stipulated by the Purchaser and confirms in writing that is no longer holds or possess any Purchaser Information.

1.9.2 Unless otherwise permitted under the terms of the agreement with the Purchaser and where the Purchase has requested the deletion of Purchaser Information, the Supplier shall ensure that, prior to disposal or decommissioning, a suitable software data wiping solution is used to permanently delete all Purchaser Information in its possession so that it cannot be restored. Where requested by the Purchaser, the Supplier shall provide the Purchaser with a certificate of destruction signed by an authorised signatory of the Supplier confirming the Supplier's compliance with this paragraph.

1.9.3 Notwithstanding paragraph 1.9.1, the Supplier may retain Purchaser Information only to the extent, and for such period, as required by law provided always that Supplier shall ensure the security and confidentiality of all such Purchaser Information and shall ensure that such Purchaser Information is only used as necessary for the purpose(s) specified in the applicable law and for no other purpose.

1.10 Access Management

In respect of electronic devices, information systems and/or IT networks that hold, store, process or are otherwise used to access Purchaser Information, the Supplier shall maintain an up-to-date list of authorised user accounts and make that list available to the Purchaser immediately on request.

1.11 Business Continuity Plan

1.11.1 The Supplier shall ensure that it has a well-defined business continuity plan ('**BCP**') in place that meets all requirements specified and/or agreed with the Purchaser or if none are specified, is in line with Good Industry Practice and, if required by the Purchaser, is provided to the Purchaser within 7 days of the Purchaser's request. The BCP shall, without limitation, include i) an appropriate data backup schedule, ii) identification of an offsite location where data backups are held in an encrypted/secure form, iii) a prompt data restoration timeframe and iv) an appropriate testing schedule to confirm the BCP is effective. The Supplier shall review and test the effectiveness of the BCP at least annually and, where requested, provide the Purchaser with evidence of the effectiveness of the BCP. Any changes that the Supplier wishes to make to the BCP must not adversely affect the security and integrity of Purchaser Information and shall be notified to the Purchaser in writing in advance of such changes being implemented.

1.11.2 The Supplier shall implement technical controls and disaster recovery processes to manage and mitigate the impact of potential loss, corruption, damage or unavailability of Purchaser Information due to unforeseen circumstances (including fire, flood and power outages) in line with the recovery time scales specified by the Purchaser in the BCP or, if none are specified, in line with Good Industry Practice.

1.12 Data Restoration

At the request of the Purchaser and in accordance with the BCP, the Supplier shall, in respect of Purchaser Information which it holds and is responsible for, restore or recreate Purchaser Information that has been lost, corrupted, damaged or destroyed. Such restoration or recreation shall be carried out at the Supplier's own cost within the timeframes set out in the BCP or, if no time frames have been agreed, within forty-eight (48) hours of the Purchaser's request.

1.13 Data Integrity

1.13.1 The Supplier shall implement as a minimum an industry standard encryption solution when transmitting or electronically accessing Purchaser Information via a communications network (e.g. Transport Layer Security (TLS) protocol).

1.13.2 The Supplier shall ensure that Purchaser Information is hosted in and accessed by Permitted Parties from only the geographical location(s) pre-approved by the Purchaser. The Supplier shall ensure that all electronic devices, information systems and/or IT networks that hold, store, process or are otherwise used to access Purchaser Information cannot be accessed by unauthorised persons.

1.14 Email

The Supplier shall ensure that its Permitted Parties only use the Supplier's authorised email accounts when dealing with the Purchaser or when emailing Purchaser Information.

1.15 Intrusion Detection & Prevention

The Supplier shall implement and maintain industry standard intrusion detection systems (IDS) and intrusion prevention systems (IPS) and provide details of the same to the Purchaser immediately upon request.

1.16 Vulnerability Scanning

The Supplier shall either:

(a) carry out a vulnerability scan on a monthly basis using industry standard tools, techniques and methodologies. The Supplier shall, within ten (10) days of it conducting a vulnerability scan, provide the Purchaser with the results of the scan; or

(b) permit the Purchaser (or its authorised representatives) to perform regular vulnerability scans on request but no more frequently than once in any calendar month.

1.17 Penetration Testing

1.17.1 The Supplier shall appoint an independent third party, which is either accredited to conduct Cyber Essentials Plus assessments or which is approved by the Purchaser in advance, to conduct a security penetration test at least annually and, additionally, following any major technology systems or infrastructure change by the Supplier. The Supplier shall, within ten (10) days of its receipt, provide a copy of the third party penetration report (along with the results of the penetration tests conducted) to the Purchaser.

1.17.2 The Supplier shall remedy any issues identified in the third party's report within the following timescales:

(a) Critical issues to be resolved immediately

(b) High risk issues to be resolved within ten (10) days

(c) Medium risk issues to be resolved within one (1) month

(d) Low risk issues to be resolved within three (3) months

The independent third party must assign a risk level based on the above for all issues identified in its report.

1.17.3 The Supplier shall instruct the same independent third party to conduct a subsequent penetration report once the Supplier has remedied all critical issues and/or high risk issues. The Supplier shall, within ten (10) days of its receipt, provide the Purchaser with an updated report to confirm the issues have been adequately resolved.

1.18 Wireless Networks

1.18.1 The Supplier shall install and operate its wireless network connections in an appropriately secure manner and in particular:

(a) access from the wireless LAN environment to the wired LAN/WAN services shall be subject to strong authentication;

(b) a Virtual Private Network (VPN) should be used with all wireless LAN installations;

(c) WPS (Wi-Fi Protected Setup) must be enabled on wireless LANs (WEP must not be used);

(d) all default passwords associated with access points or other equipment associated with the wireless LAN shall be changed from their default settings;

(e) the SSID associated with any wireless LAN must not make it obvious that it is the Purchaser's wireless LAN and, where possible, beacon frame transmission and SSID broadcast shall be disabled; and

(f) ad-hoc/peer-to-peer wireless networking capability shall be disabled on all clients.

1.19 Data Integrity (Enhanced)

The Supplier shall, as a minimum, implement and maintain an industry standard encryption solution to securely protect Purchaser Information whilst at rest.

1.20 Forensic Readiness

The Supplier shall implement a forensic readiness plan along with technical measures and processes to enable an effective investigation into any Security Incident, which shall include, without limitation, capabilities to trace an individual user's activity or use of a specific system resource, conduct root cause analysis and forensic evidence gathering.

1.21 Multi-Factor Authentication

The Supplier shall ensure all administrative access to any electronic devices, information systems and/or communication networks that hold, store, process or are otherwise used to access Purchaser Information over the Internet must use multi-factor authentication and via a cryptographically protected communications protocol.