3 - IT Security (For requirements please see Appendix B – IT Security)

Question;

3a. Please state what, if any, form of assessment in relation to the Government backed Cyber Essentials Scheme has been performed or provide details of any cyber essentials accreditation that you are planning in the future.

Cyber Essential self-assessment Aug-23.

Cyber Essentials Plus external re-accreditation assessment scheduled Oct-23.

3b. Please provide details of the controls and processes you have in place covering patching, malware (anti-virus), boundary/network security (intruder detection), content checking/blocking (filters), lockdown (prevention), and how regularly you update them.

Patching – Software Update and Patching Policy covers the review and regular deployment of patches. It is the responsibility of the user to whom the system is allocated to ensure that patches are regularly applied rapidly. Patches are automatically applied to the system on a monthly basis, but on occasion when a critical update is released users may be asked to manually apply patches.

Malware – The mandated use of anti-virus/malware tools are included in the IT Security & Utilisation policy and states the Company's designated anti-virus software must be installed on all computers and these must be regularly connected to the network to ensure that the software and security remains up-to-date. In addition to anti-virus/malware tools installed on computers, additional steps such as email and web filtering are also in place.

Boundary/network security – Sepura makes use of Firewall technologies to protect internal computer resources from devices on the internet. Firewalls are also used to segregate traffic due to sensitivity or risk and to ensure that only approved associated business units have access. Firewall rules are used to block or allow access from a source to a destination on the network. By default, all traffic that attempts to traverse the firewall is blocked by a deny rule. Access through the firewall is only possible via an explicit firewall rule where the source and destination are specified. Enhanced firewall capabilities such as Intruder Prevention System and Intruder Detection System functions are employed on the Sepura firewall. A network monitoring system [redacted]) that uses artificial intelligence is deployed to highlight unusual activity on the Sepura network.

Content checking/blocking – 3rd party email hygiene and web hygiene technologies are employed to check content and block malicious or inappropriate content.

Lockdown – Sepura's compute environment consists of numerous information assets that range in sensitivity and confidentiality. The level of security and risk mitigation applied to these assets increases in line with their sensitivity. The approach used to secure a desktop PC on the company's corporate network would differ significantly from a system containing commercially sensitive assets. Securing a sensitive information asset would follow the guidelines from the CESG / NCSC and the Center for Internet Security. Key approaches adopted across all systems include:

Data in transit – An [redacted] is used to secure communications between remote / travelling workers and the corporate network.

Data at rest – File-level encryption technologies are used to secure commercially sensitive data stored on laptops. Whole Disk Encryption technologies that meet the government's classification of Official are employed to secure more sensitive information assets.

Authentication – User accounts have strong and complex passwords for authentication to the desktop platform, with two-factor authentication to secure remote access to the corporate network.

Malicious code detection and prevention – A multi-layered defence including end-point antivirus, cloud scanning of all HTTP and HTTPS traffic and hosted message hygiene services are employed to detect malicious code. All Internet traffic passes through a stringent rule base on the corporate firewall with Intruder Prevention System functionality used to protect against zero-day vulnerabilities.

Security policy enforcement – Security settings are automatically applied to all corporate computers via Group Policy, which cannot be modified by unprivileged users. Mobile Device Management solution is employed to apply security policy and encryption to devices synchronising with the corporate email infrastructure.

Devices updates – Windows Update Service is used to automatically update download and install patches based on a corporate policy.

3c. Please provide details of the overall security and access control policy of your systems covering physical and electronic assets (including communications connection equipment, e.g. bridge, routers, patch panels). You should record details of the formal registration/deregistration process, how users are Authorised, Authenticated and held Accountable for their actions. Also include details of the measures in place to manage privilege access e.g. System Administrators and remote users.

Sepura take physical and data security seriously and have a number of policies and controls to ensure good governance. Examples of these are outlined below:

Staff Responsibilities:

Staff must not knowingly create, copy, store, transmit, publish, view, display or download messages or material from whatever source that may place the Company at risk from prosecution, civil action, embarrassment, loss of reputation or impact adversely on staff, customers or partners. This includes, but is not limited to, defamatory, obscene, pornographic, discriminatory, or abusive or otherwise inflammatory messages and material.

All staff are responsible for adhering to the requirements published in this policy and ensuring that they behave in such a way as not to compromise the security or the reputation of the Company and others. Failure to abide by this policy (as amended from time to time) will be considered to be misconduct or gross misconduct and will be treated as a disciplinary matter which may result in dismissal under the SL-HR-051 Disciplinary Policy & Procedure.

User Identification

Each user is allocated an individual username and password. Network security is individually assigned to that user account; therefore on no account should individuals allow or encourage the use of this log-in by others to access any file, account, or system. The owner of a particular username will be held responsible for all actions performed using this username.

Staff change

Managers must notify IT of staff changes that might affect security. An example of this would be an individual who has access to restricted confidential information and moves to another role where this access is not required.

Access permissions

Staff should only access electronic information and data that they require to perform their duties, while we will try to grant the appropriate permission to limit access, users should not seek access to other information outside this remit. It is the responsibility of the user to inform IT immediately if they find they are able to access other sensitive information. Access to resources is controlled via group, the process for adding someone to a group involves raising an IT request, seeking approval (and recording approval) from the group owner and then adding the user to the group.

Access to the server room

Access to the server room is restricted to members of the IT Department, Facilities, Security and First Aiders. If access is required by contractors or other staff members they must be accompanied by a member of the IT staff at all times. Entry to the server room is controlled by access cards with the appropriate permissions. The server room door must be kept locked at all times when no IT personnel are working in the room.

Acceptable Use Policy (User Directives)

As part of the new starter process, user directives must be signed which include:

General conditions

1 As the owner of a User-Id, you are responsible for its use.

2 For security reasons you should log off or lock your screen when you stop working at a terminal/PC. IT reserves the right to log off or lock any unattended screen which is left logged into the network.

3 The company reserves the right to monitor your use of company equipment and systems, including accessing any data or software thereon, except (for staff outside the UK) where restrictions exist according to National law.

4 Department Management is responsible for advising the IT Department when users of the system leave the company.

5 You are responsible for the security and backup of all data not held on the central servers.

6 Laptop users are responsible for the security of their hardware, software and data at all times.

Users MUST

7 Read, comply and observe the guidelines, responsibilities and your obligations as stated in the IT Security & Utilisation Policy (SL-IT-007) and IT Acceptable Use Policy (SL-IT-023).

8 Use Company computing facilities/software/data only for legitimate company purposes; following the company guidelines and procedures.

9 Protect access to company facilities (including HW and SW) in accordance with the company IT Security Policy.

10 Comply with the Data Protection Act (1998) if your system is used to hold personal data, e.g. names and addresses.

11 Report immediately, through the IT Help Desk (log a call), any irregular or incorrect use of the company's IT equipment or systems.

12 Advise IT of software you want (authorised by Sepura) to install on a terminal/PC including updates and patches, etc. *It is IT's responsibility to control the installation of all software on Company computing equipment.*

Users MUST NOT

13 Share your user identification (ID) with any other user. It is for personal use only.

14 Make your password known to any other person, nor let it be visible in the vicinity of the terminal /workstation / PC. *This does not apply to the situation where the IT Department is requested to solve the issue raised by the user and subsequently requires a password to access the account.*

15 Log in to the company network or equipment where your activity or connection method is not secure.

16 Connect unauthorised equipment to the network or terminals/workstations/PCs connected to the network.

17 Use any unauthorised, illegal or unlicensed software or data on company computers (if you require the use of software which is not currently approved, you should submit details and justification to the IT team for approval BEFORE installation).

Other NOTES / GUIDANCE

1 Reasonable use of the internet is tolerated subject to individual line managers' agreement, providing it is not excessive and does not degrade your productivity or interfere with any business priorities.

2 On no occasion it is considered acceptable to view or download any material from the Internet that the company considers indecent, illegal, or offensive.

3d. Please provide details of how your security and access control policy complies with the Security Policy Framework (including where necessary, use and control of backup systems, network storage and segregation of HMRC data (including 'cloud' solutions), and additional security for more sensitive information assets).

Sepura operates a number of policies and procedures that align with the Security Policy Framework.

The Business Risks and Opportunities process is used to identify Risks and Opportunities, in order to:

Prevent, or reduce, undesired effects.

Enhance desirable effects.

Deliver improvements.

Provide assurance that the business can achieve its intended results.

The information security policy sets out the requirement to preserve confidentiality, integrity and availability of all the physical and electronic information assets throughout the organization in order to preserve our competitive edge, cash flow, profitability, legal, regulatory and contractual compliance and commercial image.

The data classification policy ensures the security of data by assisting Sepura employees in determining the correct classification of data, and the subsequent availability, distribution, and storage.

The Information asset risk assessment process helps identify risks that could negatively impact our organisation's ability to conduct business and provides a mechanism to assess information security risks with regard to the potential impact on the business. For assets deemed as a high risk, the process outlines steps to mitigate risk or record on the risk register for review by the Security Risk Management Team.

The Sepura Backup Policy states that all data within IT Systems shall be protected against loss or corruption through the use of robust and regular backup procedures to ensure that the organisation is not significantly disrupted should a failure occur within the system.

The Access Control Policy (Building 9000) states that physical access control and site security are vital to the business. Building 9000 is a List X registered site. The procedure outlines the processes which Sepura Employees and non-Sepura personnel should follow when accessing the building and moving within the

Sepura Security ring fence. The policy references restricted areas and includes the use of ID badges and colour-coded lanyards to signify security vetting levels and for contractors/visitors.

3e. Please describe how you ensure all software and data is approved before being installed, and how your information systems are reviewed for compliance with security implementation standards (e.g. penetration testing).

Sepura's IT Security & Utilisation policy specifies the management and audit of Software.

7.2 Software

Software licensing, application compatibility and application support need to be carefully managed to maintain compliance and ensure that system performance is maintained.

7.2.1 Licenced software

Licenced software must not be copied, removed or transferred to any equipment without written authorisation from the IT Department.

7.2.2 Authorised software

Only software that has been authorised by the IT Department (this includes any freeware or shareware) may be used on PCs and laptop computers connected to the Sepura IT network.

7.2.3 Audits of desktop software

Audits of desktop software may occur, and the presence of unauthorised software will be investigated. Sepura reserves the right to remove any files or data from IT systems, especially any information it views as offensive, prejudicial to the Company or its staff or illegal, including any software for which a valid licence cannot be produced.

3f. Please provide details of the controls and processes (including level of encryption and controlled access procedures) you have in place for the use of portable media and storage devices exceptionally loaded with HMRC data.

Portable media is not used for the handling or loading of HMRC data.

3g. Please provide details of how all equipment (e.g. hardware, portable media) that holds or has held data will be destroyed or decommissioned, and how all data will be rendered unreadable and irretrievable in line with HMG Security Policy Framework requirements for information management.

The IT Security & Utilisation policy that must be read and agreed to by all employees' states:

"PCs and laptops for disposal must have the hard disk 'wiped clean' or destroyed before they are distributed outside Sepura. Hard disks are kept under IT possession and destroyed to avoid any data access."

The WEEI Disposal instruction document requires that all hard drives must be removed from the PCs, laptops and servers before the equipment is taken for disposal, with the hard drives being disposed of separately.

Drives and tapes are rendered unusable prior to them leaving the premises, once off-site the media (drives and tapes) are shredded using a certified data destruction specialist.

The Disposal/Destruction of returned equipment policy includes the below statement:
“4 ENCRYPTED AND NON-ENCRYPTED EQUIPMENT RETURNED FOR DESTRUCTION/DISPOSAL
Additionally, in order to meet the combined requirements of the UK network provider (Airwave), Home Office, NCSC and ETSI for Terminals and Hardware that are classified as [redacted] there needs to be special measures taken. Disposal of all terminals and peripherals is handled via the Sepura Service Centre and this service adheres to relevant environmental legislation and specific regulations linked to Airwave terminals. The other parts of the radios including batteries are separately recovered and recycled through an approved third party.”