Security Policy (LO073)

1. Scope

1.1 This policy defines a structure by which Shield Environmental Services Ltd (SES) computer systems, assets, infrastructure and computing environment will be protected from threats both internally and externally as well as accidental or purposeful contravention of this policy.

2. Core Principles

2.1 All central computer systems, environments and information contained within them will be protected against unauthorised access.

2.2 Information kept within these systems will be managed securely, to comply with relevant data protection laws and to satisfy the Company's expectations that stated assets will be managed in a professional, safe and responsible manner.

2.3 All employees of the Company are required to familiarise themselves with this policy, to adhere to it and comply with its requirements.

2.4 Senior management has a responsibility for ensuring the implementation of, adherence to and compliance with this policy throughout their areas of functional responsibility.

2.5 The integrity of all central computer systems, the confidentiality of any information contained within or accessible on or via these systems is the responsibility of Shield Environmental Services Ltd (SES).

2.6 All regulatory and legislative requirements regarding computer security and IT based information confidentiality and integrity will be addressed by Shield Environmental Services Ltd (SES).

2.7 All breaches of security will be reported to and initially investigated by SES.

2.8 All users have a responsibility to report promptly (to SES and the external IT consultant SHG) any incidents which may have an IT security implication for the Company.

3. The IT Environment

3.1 SES manages, maintains and operates a range of central computing servers, systems, backup systems and the overall network infrastructure interconnecting these systems.

3.2 The IT Environment is defined as all central computing resources and network infrastructure managed and overseen by SES and all computing devices that can physically connect to it, and have been authorised to connect to this environment. All are covered by this policy, including computing hardware and software, any Company related data residing on these machines or accessible from these machines within the site network environment and any media such as CD-ROMs, DVD-ROMs and portable storage devices.

3.3 All temporary and permanent connections via the Company network, casual laptop docking points, the Wireless network(s), the Virtual Private Network (VPN) and remote desktop connection are similarly subject to the conditions of this policy.

3.4 Computing resources not owned by the Company may be connected to the Company's network. However, all such resources must comply with Company Guidance governing the use of computing resources.

3.5 SES reserves the right to monitor, log, collect and analyze the content of all transmissions on networks maintained by SES using an external IT consultancy (SHG) at any time deemed necessary for performance, fault diagnostic and IT compliance purposes.

4. Physical Security

4.1 SES provides secure machine room facilities with protected power arrangements and climate controlled environments. Although primarily for the provision of central computing and network facilities, individual branches and, if appropriate, individuals are encouraged to consult SES where they have local systems in less than comparable environments with a view to those systems being housed in the SES Head Office Machine Room.

4.2 Any computer equipment in general office environments should be secured behind locked doors or protected by user log-out and or password protected screensavers whenever it is left unattended.

4.3 Desktop machines in public areas should contain a device or mechanism for securing and protecting the main components and contents of the computer from theft.

4.4 Any portable equipment (such as laptops, memory sticks, CDs, PDAs etc) should use a log-on or power-on password wherever possible. Any unattended portable equipment should be physically secure, for example locked in an office or a desk drawer. When being transported in a vehicle they should be hidden from view. Employees should avoid storing sensitive information on portable equipment whenever possible (see section 5. Data Security).

4.5 Employees who store confidential information on Company owned portable equipment must ensure that such data is thoroughly and securely cleansed from that equipment when they leave the Company's employment, once a backup has been completed. Employees should consult the SES external IT consultant (SHG) for assistance and guidance on appropriate cleansing techniques and tools.

5. Data Security

5.1 The Company attaches great importance to the secure management of the data it holds and generates and will hold employees accountable for any inappropriate mismanagement or loss of it.

5.2 The Company holds a variety of sensitive data including personal information about employees. If you have been given access to this information, you are reminded of your responsibilities under the form Data control policy (LO070). Alternatively, please contact the specified Data Controller for further details.

5.3 The Company provides secure and practical remote access to information and data held within its various systems environments and IT infrastructure. In most cases, gaining access to such data from an offsite point of electronic access will prove sufficient and safe for most needs and is the recommended general mode of remote use of such data and information.

5.4 Any copying or original generation of sensitive data and information onto any form of portable media transport device or mechanism (Memory Stick, CD, DVD, External Hard Drive, PDA, portable music player, Laptop, etc.) or its transportation beyond the secure environment it was intended to be used within (systems environment, PC environment, site, office etc.) carries additional responsibilities for the individual undertaking such activity.

5.5 These responsibilities should be clarified by performing a risk analysis, which considers the following rules/principles:

5.5.1 Employee (personal) data should never leave the site. In this context leave implies its physical transport to an external and insecure location. Remote access to such data through an individuals approved access levels and permissions is distinct and not intended to be included in the term leave.

5.5.2 If it is a unique or master version of data/information that has not been safely copied to a secure electronic or physical location or environment within the Company's IT Environment (implying that its subsequent loss is irrecoverable) then a copy should be made and stored securely prior to its offsite transportation for use.

5.6 If, following such a risk analysis, an individual identifies an imperative to take sensitive data off site (in any media form) they are not to do so without prior consultation with SES senior management. Suitable encryption solutions can be provided by SES external IT consultant (SHG) for the data prior to its removal from site. Failure to comply with this requirement will be considered a serious breach of this policy.

5.7 In respect to the SES client portal login section of the website (http://www.shieldenvironmental.co.uk**) all logins are secured via e-Commerce industry standard encrypted SSL connection.**

5.8 Client portal data is held with an external hosting facility (Rackspace), which complies with the relevant IT security standards e.g. ISO 27001. The system is audited annually for any potential security issues as part of their on-going accreditation. SES are able to provide relevant hosting facility certification where necessary to satisfy client security checks.

5.9 Where reasonably practicable SES will seek to ensure that all client portal data is stored within the EEU unless otherwise stated by the client. This will be included as part of any contract tender for external data hosting.

5.10 SES will work with clients where requested to do so, to ensure system and web browser compatibility prior to full launch of their client portal login.

5.11 SES maintains a strict data permission hierarchy in which all requests for access to/transfer of sensitive data, both internally and externally, in the first instance must be made to senior management who will make an executive decision on the access/transfer of the data. Senior management may choose to contact SHG directly to discuss the permissions or delegate this to the Data Controller. The Data Controller under the DPA 2018 **for SES will be informed of the decision to access/transfer data and a record kept of the details of the access/transfer. At no time will SES employees be allowed to access/transfer sensitive data without the permission of senior management. Contravention of this clause may be treated as a loss or theft as per section 6. Loss or Theft of Confidential Information and dealt with appropriately.**

6. Loss or Theft of Confidential Information

6.1 All incidences of loss or theft of confidential information should be reported so that they may be investigated. A data or IT security incident relating to breaches of security and/or confidentiality could range from computer users sharing passwords to the loss or theft of confidential information either inside or outside the Company.

6.2 A security incident is any event that has resulted or could result in:

6.2.1 The disclosure of confidential information to any unauthorised person.

6.2.2 The integrity of the system or data being put at risk.

6.2.3 The availability of the system or information being put at risk.

6.2.4 Adverse impact, e.g.

6.2.4.1 Negative impact on the reputation of the Company.

6.2.4.2 Threat to personal safety or privacy.

6.2.4.3 Legal obligation or penalty.

6.2.4.4 Financial loss or disruption of activities.

6.3 All incidents must be reported to your immediate line manager and to SES senior management. Serious incidents should be reported immediately to the Managing Director and Technical Director. A written report should be submitted containing the following information:

6.3.1 Details of the incident.

6.3.2 Date of discovery of the incident.

6.3.3 Place of the incident.

6.3.4 Who discovered the incident.

6.3.5 Category/classification of the incident.

6.3.6 Action already taken if risk to organisation.

6.3.7 Any action taken by the person discovering the incident at the time of discovery, e.g. report to police.

6.4 In the case of a serious potential breach, the Technical Director will instigate an investigation into the incident and will decide whether it needs to be reported to any regulatory bodies or other third parties, e.g. insurers. The Technical Director will retain a central register of all such incidents occurring within the Company.

6.5 The following is a list of examples of breaches of security and breaches of confidentiality. This list is not exhaustive and should be used as a guide only. If there is any doubt as to what constitutes an incident, it is better to inform the Technical Compliance Department who will then decide whether a report should be made.

6.6 Examples of breach of security:-

6.6.1 Loss of computer equipment due to crime of carelessness.

6.6.2 Loss of portable media devices, e.g. memory sticks etc.

6.6.3 Accessing any part of a database using someone else's password.

6.6.4 Finding evidence of forced entry into an area in which computer equipment exists.

6.7 Examples of a breach of confidentiality:

6.7.1 Finding confidential/personal information either in hard copy or on a portable media device outside Company premises or in any of the Company's common areas.

6.7.2 Finding any records about employees in any location outside the Company's premises.

6.7.3 Passing information to unauthorised people either verbally, written or electronically.

7. Specific Systems

7.1 Email

7.1.1 Email is not an entirely secure medium. You should be conscious of this and consider how emails might be used by others. Remember that emails can easily be taken out of context and that once an email is sent you cannot control what the recipients might do with it. Employees should be aware that email is an especially quick method of transmitting large quantities of data, often in an uncontrolled manner.

7.1.2 Similarly you should not necessarily trust the information received in an email; in particular, you must never respond to an email request to give a username or password.

7.1.3 Attachment file sizes should be kept to the minimum where practicable in order to reduce memory demand on both internal and external email systems as well as physical server memory.

7.2 File Storage

7.2.1 All users have access to the centrally managed file storage.

7.2.2 For the vast majority of applications the security of files stored centrally is appropriate. In particular this means they will be backed up. However if your files require a higher level of security, please contact SHG.

7.3 The Web

7.3.1 Users should consider the security implications of any information they put on the Company's web-site, and the Company reserves the right to remove any material which it deems inappropriate, illegal or offensive.

7.3.2 Users shall not in any way use web space to publish material which undermines IT security at the Company. In particular this covers making information available about how IT security is implemented at a practical level, or any known weaknesses.

7.3.3 Web based data collection will be subject to the same data security protocols as outlined in section 5. Data Security.

7.4 Company Network

7.4.1 Individuals must seek permission from local support representatives before connecting any machine to the LAN. SHG may disconnect any unauthorised host from the network without warning.

7.5 Remote Access to Systems

7.5.1 Remote access is defined as accessing systems from a physically separate network. This may include:

7.5.1.1 Connections direct across the Internet

7.5.1.2 VPN Connections

7.5.2 Any user with a valid Company computer account may access systems as appropriate. Remote access is allowed via secure methods only. Remote connections to any site IT services are subject to the same rules and regulations, policies and practices just as if they were physically on the site. SHG shall provide the only VPN that may be used.

7.5.3 All connections via these services will be logged. No other remote access service shall be installed or set up, including single modems connected to servers or workstations. Any active dial-in services found to be in existence will be removed from the network.

7.6 Anti-Virus Security

7.6.1 SHG will provide means by which all users can download and install current versions of site-licensed virus protection software. In relation to SES this is Sophos Endpoint Security and Control.

7.6.2 Users must ensure that they are running with adequate and up-to-date anti-virus software at all times. If any user suspects viral infection on their machine, a complete virus scan should be performed. If SHG detect a machine behaving abnormally due to a possible viral infection it will be disconnected from the network until deemed safe. Reconnection will usually only be after liaison with local IT support.

8. Software Installation

8.1 SES uses SHG IT consultants to manage software installation across the IT system, including all offices as well as portable equipment. In this instance smart mobile phones with the capacity to run applications will be treated as portable equipment. This control is designed to keep the IT system, thus sensitive data contained within safe and secure. Users wishing to install specific software must in the first instance make their request to the Data Controller or senior management dependent on the technical/financial implications of the software. If the software is approved, the Data Controller will liaise with SHG to install the software in a manner compliant with this policy.

9. Related Documentation

Data control policy (LO070)
Privacy policy (LO072)

10. Management Representative

Date: 15/03/2018

Name: Katy Webster

Position: Procurement Manager

Signature: