Information Security Policy

Version	1.0
Status	Final
Document Owner	Technology Lead

Document information

Document type	Policy
Review frequency	Annual
Reviewer	Technology Lead
Approver	Billel Ridelle
Next review date	April 2020
Scope	Sweep – whole company

Authoring history

Version	Date:	Description:	Author
0.1	27/02/2019	Initial draft for discussion	Nicolas Guerin
1.0	05/03/2019	First version	Nicolas Guerin

Review and approval history

Version	Date	Description	Reviewer / approver
1.0	05/03/2019	Initial approved version	CEO

Distribution	Communicated during induction and available on the shared drive.

Contents

1 Introduction

This information security policy is a key component of Sweep management framework. It sets the requirements and responsibilities for maintaining the security of information within Sweep. This policy may be supported by other policies and by guidance documents to assist putting the policy into practice day-to-day.

This policy applies to anyone who has a business need to handle Sweep's information or equipment, including all employees, contractors, consultants and business partners.

2 Aim and Scope of this policy

The aims of this policy are to set out the rules governing the secure management of our information assets by:

- preserving the **confidentiality, integrity and availability** of our business information;
- ensuring that all members of staff are aware of and fully comply with the relevant **legislation** as described in this and other policies;
- ensuring an approach to security in which all members of staff fully understand their own **responsibilities;**
- creating and maintaining within the organisation a level of **awareness** of the need for information;
- detailing how to **protect** the information assets under our control.

This policy applies to all information/data, information systems, networks, applications, locations and staff, including contractors, consultants and business partners.

3 Responsibilities

Ultimate responsibility for information security rests with the Sweep Chief Executive Officer (CEO), but on a day-to-day basis the Technology Lead (Tech Lead) shall be responsible for managing and implementing the policy and related procedures.

Responsibility for maintaining this Policy, the business Information Risk Register and for recommending appropriate risk management measures is held by Tech Lead. Both the Policy and the Risk Register shall be reviewed by the CEO at least annually.

Line Managers are responsible for ensuring that their permanent staff, temporary staff and contractors are aware of:

- the information security policies applicable in their work areas
- their personal responsibilities for information security
- how to access advice on information security matters

All staff shall comply with the information security policy and must understand their responsibilities to protect the company's data. Failure to do so may result in disciplinary action.

Line managers shall be individually responsible for the security of information within their business area.

Each member of staff shall be responsible for the operational security of the information systems they use.

Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

Access to the organisation's information systems by external parties shall only be allowed where a contract that requires compliance with this information security policy is in place. Such a contract shall require that the staff or sub-contractors of the external organisation comply with all appropriate security policies.

4 Legislation

Sweep is required to abide by certain UK, European Union and international legislation. It also may be required to comply to certain industry rules and regulations.

The requirement to comply with legislation shall be devolved to employees and agents, who may be held personally accountable for any breaches of information security for which they are responsible.

In particular, Sweep is required to comply with:

- The Data Protection Act (2018);
- The Copyright, Designs and Patents Act (1988);
- The Computer Misuse Act (1990);
- The Health and Safety at Work Act (1974);
- Human Rights Act (1998); and
- Regulation of Investigatory Powers Act 2000.

5 Personnel Security

5.1 Contracts of Employment

Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a security and confidentiality clause.

References for new staff shall be verified and a passport, driving license or other document shall be provided to confirm identity.

Information security expectations of staff shall be included within appropriate job definitions.

Whenever a staff member leaves the company their accounts will be disabled the same day they leave.

5.2 Information Security Awareness and Training

The aim of the training and awareness programmes are to ensure that the risks presented to information by staff errors and by bad practice are reduced.

Information security awareness training shall be included in the staff induction process and shall be carried out annually for all staff

An on-going awareness programme shall be established and maintained in order to ensure that staff awareness of information security is maintained and updated as necessary.

5.3 Intellectual Property Rights

Sweep shall ensure that all software is properly licensed and approved by the Tech Lead. Individual and Sweep's intellectual property rights shall be protected at all times.

Users breaching this requirement may be subject to disciplinary action.

6 Access Management

6.1 Physical Access

Only authorised personnel who have a valid and approved business need shall be given access to areas containing information systems or stored data.

6.2 Identity and passwords

Passwords must offer an adequate level of security to protect systems and data

All passwords shall be ten characters or longer and contain at least two of the following: uppercase letters, lowercase letters and numbers

All administrator-level passwords shall be changed at least every 90 days.

Where available, two-factor authentication shall be used to provide additional security.

All users shall use uniquely named user accounts.

Generic user accounts that are used by more than one person or service shall not be used.

6.3 User Access

Access to information shall be based on the principle of “least privilege” and restricted to authorised users who have a business need to access the information.

6.4 Administrator-level access

Administrator-level access shall only be provided to individuals with a business need who have been authorised by the Tech Lead.

A list of individuals with administrator-level access shall be held by the Tech Lead and shall be reviewed at least annually.

Administrator-level accounts shall not be used for day-to-day activity. Such accounts shall only be used for specific tasks requiring administrator privileges.

6.5 Application Access

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators.

Authorisation to use an application shall depend on a current licence from the supplier.

6.6 System Perimeter access (firewalls)

The boundary between business systems and the Internet shall be protected by firewalls, which shall be configured to meet the threat and continuously monitored.

All servers, computers, laptops, mobile phones and tablets shall have a firewall enabled, if such a firewall is available and accessible to the device’s operating system.

The default password on all firewalls shall be changed to a new password that complies to the password requirements in this policy, and shall be changed regularly

All firewalls shall be configured to block all incoming connections.

If a port is required to be opened for a valid business reason, the change shall be authorised following the system change control process. The port shall be closed when there is no longer a business reason for it to remain open.

6.7 Monitoring System Access and Use

An audit trail of system access and data use by staff shall be maintained wherever practical and reviewed on a regular basis.

The business reserves the right to monitor and systems or communications activity where it suspects that there has been a breach of policy in accordance with the Regulation of Investigatory Powers Act (2000).

7 Asset Management

7.1 Asset Handling

By default, all business information is considered as confidential. After approval from the Tech Lead or the CEO, an information can be reclassified as public and can be made available publicly through any channels.

Common examples of public information are:

- Details of products and services on the website;
- Published company information;
- Social media updates; or
- Press releases.

All staff are responsible for handling information assets in accordance with this security policy, especially any information defined as “sensitive personal data” under the Data Protection Act.

7.2 Removable media

Removable media (such as USB memory sticks and recordable CDs/DVDs) are not allowed to store business data.

Removable media of all types that contain software or data from external sources, or that has been used on external equipment, require the approval of the Tech Lead before they may be used on business systems. Such media must be scanned by anti-virus before being used.

Where indicated by the risk assessment, systems shall be prevented from using removable media.

Users breaching these requirements may be subject to disciplinary action.

7.3 Mobile working

Where necessary, staff may use company-supplied mobile devices such as phones, tablets and laptops to meet their job role requirements

Use of mobile devices for business purposes (whether business-owned or personal devices) requires the approval of the Tech Lead or the CEO.

Such devices must have anti-malware software installed (if available for the device), must have PIN, password or other authentication configured, must be encrypted (if available for the device) and be capable of being remotely wiped.

Users must inform the Tech Lead or the CEO immediately if the device is lost or stolen and business information must then be remotely wiped from the device.

7.4 Personal devices / Bring Your Own Device (BYOD)

Where necessary, staff may use personal mobile phones to access business email. This usage must be authorised by the Tech Lead. The device must be configured to comply with the mobile working section and other relevant sections of this policy.

No other personal devices are to be used to access business information.

7.5 Social Media

Social media may only be used for business purposes by using official business social media accounts with authorisation from the CEO. Users of business social media accounts shall be appropriately trained and be aware of the risks of sharing sensitive information via social media.

Business social media accounts shall be protected by strong passwords in-line with the password requirements for administrator accounts.

Users shall behave responsibly while using any social media whether for business or personal use, bearing in mind that they directly or indirectly represent the company. If in doubt, consult the CEO.

Users breaching this requirement may be subject to disciplinary action.

8 Computer and Network Management

8.1 Operations Management

Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the Tech Lead.

Such procedures shall include the provision of system hardening (i.e. changing default passwords, removing unused software and accounts…).

8.2 System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the Tech Lead.

8.3 Accreditation

The organisation shall ensure that all new and modified information systems, applications and networks include security provisions.

They must be correctly sized, identify the security requirements, be compatible with existing systems according to an established systems architecture (as required) and be approved by the Tech Lead before they commence operation.

8.4 Software Management

All application software, operating systems and firmware shall be updated on a regular basis to reduce the risk presented by security vulnerabilities.

All software security updates/patches shall be installed within 14 days of their release.

Only software which has a valid business reason for its use shall be installed on devices used for business purposes.

Users shall not install software or other active code on the devices containing business information without permission from the Tech Lead.

For the avoidance of doubt, all unnecessary and unused application software shall be removed from any devices used for business purposes.

8.5 Local Data Storage

Data shall not be stored locally on the business premises, except temporarily provided that a loss would not impact any business activities.

8.6 External Cloud Services

Where data storage, applications or other services are provided by another business (e.g. a 'cloud provider') there must be independently audited, written confirmation that the provider uses data confidentiality, integrity and availability procedures which are the same as, or more comprehensive than those set out in this policy.

The agreement with the other business shall include the provision of secure backups for Sweep's data. Otherwise, an alternate and secure backup solution shall be implemented.

8.7 Protection from Malicious Software

The business shall use software countermeasures, including anti-malware, and management procedures to protect itself against the threat of malicious software.

All computers, servers, laptops, mobile phones and tablets shall have anti-malware software installed, where such anti-malware is available for the device's operating system.

All anti-malware software shall be set to:

- scan files and data on the device on a daily basis;
- scan files on-access;
- automatically check for, and install, virus definitions and updates to the software itself on a daily basis;
- block access to malicious websites.

9 Response

9.1 Information security incidents

All breaches of this policy and all other information security incidents shall be reported to the Tech Lead and the CEO.

If required, as a result of an incident, data and audit trails will be isolated to facilitate forensic examination. This decision shall be made by the CEO.

Information security incidents shall be recorded in the Security Incident Log and investigated by the Tech Lead to establish their cause and impact with a view to avoiding similar events. The risk assessment and this policy shall be updated if required to reduce the risk of a similar incident re-occurring.

9.2 Business Continuity and Disaster Recovery Plans

The organisation shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

Business continuity and disaster recovery plans shall be tested at least once a year or after major system changes.

9.3 Reporting

The Tech Lead shall keep the business informed of the information security status of the organisation by means of regular reports to senior management.

9.4 Further Information

Further information and guidance on this policy can be obtained from the Tech Lead. Comments and suggestions to improve security are always welcome.