ISMS04 - Information Security Policy

Overview

SMS Environmental Ltd has an ethical, legal and professional duty to ensure that the information it holds conforms to the principles of confidentiality, integrity and availability. The Company is responsible for safeguarding information where necessary against unauthorised disclosure. The information must be accurate, timely and accessible on a need to know basis.

This information security policy defines SMS Environmental's approach to information security management. It outlines the guidelines and responsibilities necessary to safeguard the security of the information systems. Supporting policies and procedures provide further details.

SMS Environmental is committed to preserving the confidentiality, integrity and availability of data supplied by, generated by and held on behalf of third parties for the purpose of carrying out work agreed by contract in accordance with the requirements of information security standard ISO 27001 and legislative and regulatory regulations. HR73 Privacy Policy details how SMS Environmental deals with personal data.

Scope

This policy is applicable to, and is communicated to all employees, suppliers, contractors and other relevant interested parties. This includes, but it is not limited to, any systems, networks or data outsourced by the company and any systems or data managed by the SMS Environmental internally, use of mobile devices. The scope of the SMS Environmental's information security system is the provision of water treatment and water hygiene services, including installation and maintenance, training and legionella risk assessments. The design, development and provision of compliance software. The provision of HVAC maintenance services and the management of HVAC installations in accordance with the current Statement of Applicability held on Google Drive.

Purpose

The main purpose of this policy is to:

- ensure the protection of all information systems and mitigate the risks associated with unauthorised access to confidential data, loss, misuse, damage or abuse of these systems
- ensure appropriate awareness of relevant legislations
- ensure the general awareness of information security responsibilities for confidentiality and integrity of the data
- control and monitor the processes to ensure continuous improvement

Responsibilities overview

Data Operators / End Users

- Using safeguards established by IT department
- Following policies and procedures
- Not sharing password and secret authentication information

Senior Managers and the Senior Leadership Team

- IT & Information Security Management
- Ensuring that information security objectives are established and are compatible with the strategic direction of the company
- The implications of Risks to Strategy Objectives
- Use of IT/ Information Security Risk Assessment to reduce risk in strategic moves
- Management of IT/ Information Security Management System Framework & Governance
- Acceptance of or decision on risk, based on risk assessment

IT Department

- Coordinate the development and implementation of information management practices including policies, standards, guidelines and procedures
- Monitor and report on any information intrusion incidents and activate strategies to prevent further incidents.
- Work with the Compliance Manager to ensure that information assets have been assigned appropriate security classifications.
- Defining and implementing appropriate safeguards to ensure the confidentiality, integrity, and availability of the information asset
- Assessing and monitoring safeguards to ensure their compliance and report situations of non-compliance
- Authorising access to those who have a business need for the information, implementing authorisation directive
- Ensuring access is removed from those who no longer have a business need for the information.
- Contribute to the strategic direction of information management within the organisation
- Information Security Risk Assessment – management Information Security Risks to the business
- Protect Information assets
- Day to day operational activities, support and governance responsibilities
- Compliance with the company procedures
- Reporting and logging issues/ implementing corrective actions
- Managing and maintenance of Information Security operational equipment
- Maintenance and upkeep of the asset as defined by the IT Department
- System Restart and recovery
- Implementing any changes as per the change management procedure
- Backup of the information
- Updating of information asset inventory register;

Compliance Manager

- Business Continuity Plan Controller
- Support management and maintenance of Information Security Management System, including policies and processes
- Identifying the classification level of information asset
- Information Security Risk Assessment – identification Information Security Risks to the business
- Develop policies, procedures and standards to ensure the security, confidentiality and privacy of information that is consistent with organisational Information security policy
- Review of policies and procedures in conjunction with leadership and relevant parties

Compliance Department

- Training and communication

Operational team management

- Safeguarding processes in accordance with ISO27001 and company procedures
- Reporting issues, potential problems, concerns and security breaches
- Managing and controlling operational risks related to Information Security

Further information can be found within IMS01, section 1.5 “Management Responsibility”

Organisational Context

Key activities on which SMS Environmental is dependent on, are presented in the figure below.

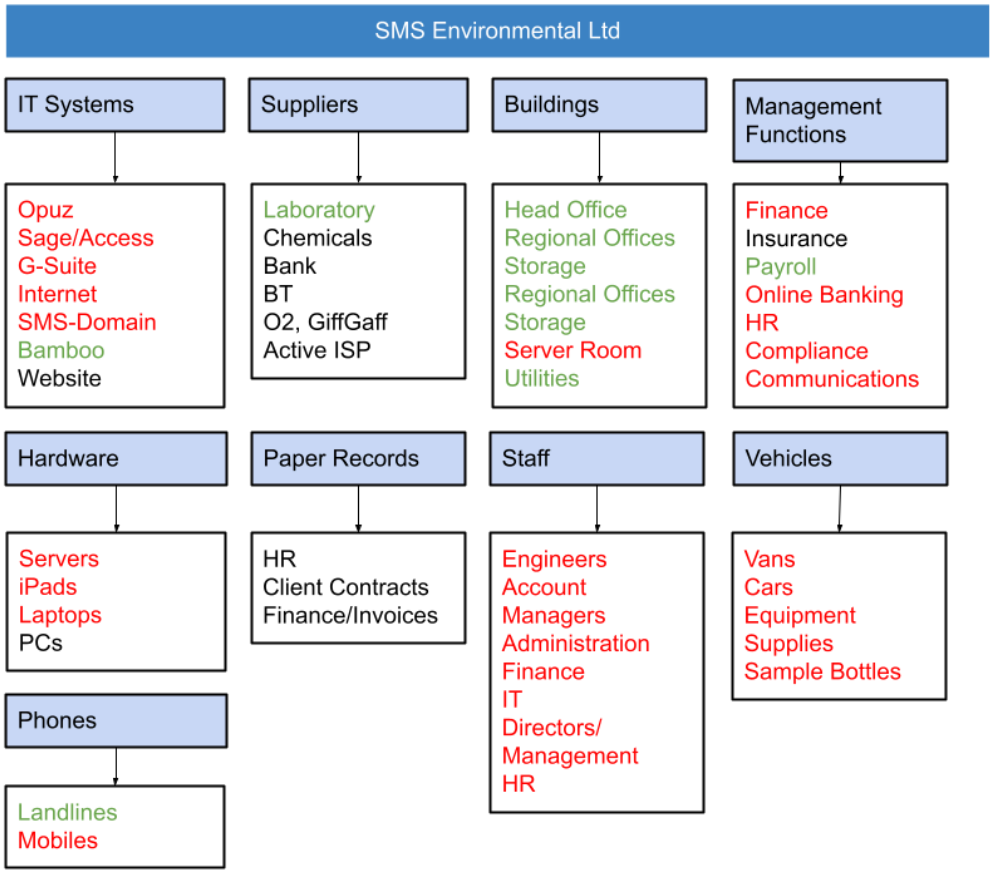

Figure 1 SMS Environmental Ltd Business Dependency Map

Key stakeholders affecting, and being affected by SMS Environmental activities are presented in the figure below.

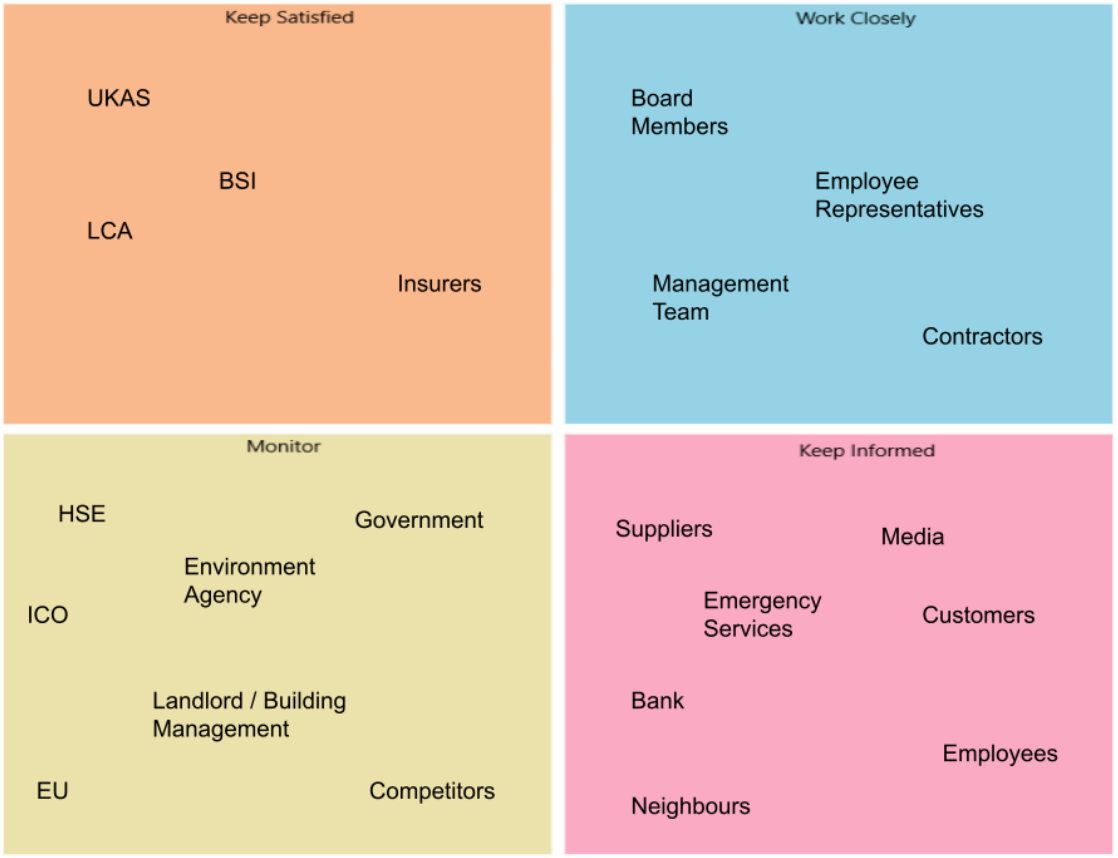

Figure 2 Identification of Stakeholders

Requirements of Interested Parties

This list also appears in IMS01.

Interested parties and their requirements, needs, and expectations relevant to the ISMS include, but are not limited to:

- Accreditation bodies
  - Compliance with requirements of relevant standards
  - Access only to required data to enable audit
  - Have sufficient skills, knowledge, and experience to effectively audit the ISMS
- Government or regulatory bodies (suggest split into separate bodies as requirements differ by ministry/department etc)
  - Comply with legal requirements and duties
- Shareholders, Board members, Senior Leadership and Management Teams
  - Maintain ownership of ISMS overview and policies
- Employees and their representatives
  - Securely store and use information, including limiting access to private or sensitive information
  - No data to be shared with other parties unless otherwise agreed

    - Sufficient training to be able to work within the ISMS
- Suppliers and contractors
    - Prompt and secure payment
    - Defined scope of works
    - Securely store and use information, including limiting access to private or sensitive information
    - No data to be shared with other parties unless otherwise agreed
- Customers or Clients
    - Comply with all data security rules, laws, and regulations
    - Comply with all contractual data security terms
    - Securely store and use information, including limiting access to private or sensitive information
    - No data to be shared with other parties unless otherwise agreed
- Opuz
    - Comply with contractual obligations between parties
- General requirements, needs, and expectations include:
    - The current and future impacts of climate change
    - Health and safety of employees, and people other than employees

Policy

Information Security Management takes responsibility for ensuring that information used, processed and stored by SMS Environmental is classified in accordance with appropriate levels of confidentiality, integrity and availability as well as relevant legislative, regulatory and contractual requirements.

Employees responsible for the management of information security systems must ensure appropriate classification of information. They are responsible for handling that information in accordance with its classification level and any associated procedures or systems.

All employees, regardless of their role and level of access and responsibility are obliged to handle information appropriately and in accordance with its classification level.

Information is protected against unauthorised access and processing in accordance with its classification level.

Information availability and access is established based on legitimate need for access on a need to know basis. Employees who have been granted access must not pass on information to others unless they have also been granted access through appropriate authorisation.

Security incidents and breaches of this policy must be reported immediately to the IT Department and Compliance Manager and dealt with in accordance with the relevant corrective action procedure.

Information Classification

Label	Access Level	Scope	Lawful Basis	Availability
Strictly Confidential	Specified only, as required	Sensitive - Personal Data Personally Identifying Data Bank details Passwords	Compliance with legal obligation	Restricted availability, information released only when authorised or required by Law or internal policy
Confidential	Specified only, as required	Personal Data Company secrets, future plans Outbreak scenarios	Compliance with legal obligation. Protection of business.	Restricted availability, information released only when authorised or required by Law or internal policy
Restricted	Employees & Clients (restricted only to client relevant data)	Internal documents, communications and correspondence Communications and correspondence with external parties Minutes Opuz system	Compliance with legal and contractual obligation	Available internally or within access permission only or as required by interested parties
Public	Full availability as required	Annual Accounts Certificates Information Available on the website	Public Interest	Freely available through website and as required

Confidential information relates to or may include, but is not inclusive of, trade secrets, certain processes, operations, methods of work, sales, purchases, identification of employees and customers, inventories, income, profits, losses, expenditures or any other information of commercial or personal value. Internal access to this information must be authorised as appropriate.

Where required (for example depending on client requirements) SMS will adopt security measures or processes required by relevant parties.

Any data, which is classified as sensitive personal data under the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR) **will be classified as confidential.**

Confidential files and emails will be preceded with 'CONFIDENTIAL' word in the email subject or file name as described in HR16 Internal Communications Policy.

Security Objectives

The Information Security Objectives ISMS19 must be reviewed at least annually and be established at various relevant functions and levels. The security objectives must be consistent with this policy, be measurable whenever possible, take into account relevant information security requirements and the results from risk assessment and risk treatment, be communicated and updated whenever there is a significant change that would affect their development and design. When establishing the objectives, the objective action, management, resources, responsibility, evaluation and the proposed completion target must be determined.

Monitoring and Measurement – performance evaluation

Information security performance – processes and controls and the effectiveness of the information security management system is measured through monitoring, measurement, analysis and evaluation. The results from monitoring and measurement shall be analysed and evaluated during ISO27001 Management

Review (SFT094 Compliance Management Review Agenda) by the following methods

Aspect	Associated Processes and controls	Method of monitoring	Frequency	Method of analysing	Responsibility
Legislation	Compliance evaluation, Compliance Management Review	ISMS05 Legal Compliance Register	6 monthly PPM	Review of compliance through: http://www.lawsociety.org.uk/support-services/advice/practice-notes/information-security/ https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/ Compliance Management Review	Compliance Team
Corrective & Improvement Actions	Internal & External Audit, Management Meetings, Management Review, Annex A – operational controls	CSIP Tasks on Opuz, Hazards,	Annual Management Meeting PPM	Review of corrective/ improvement actions, follow up actions, completion status	IT Department, Compliance Team
Changes Management	Changes/ Issues Management Control	Control of changes – ISMS13, IMS01	Annual Management Meeting PPM, IT Meetings	Annual management reviews check any completed changes tasks.	IT Department, Compliance Team
Issues Management	Changes/ Issues Management Control	Reporting procedures ISMS17 Information Security Incident Management Procedure	Annual Management Meeting PPM, IT Meetings	IT issues - agreeing follow up actions if necessary, analysing trends in incident records	IT Department, Compliance Team
Equipment	Asset Register	Inventory of Equipment on Opuz/asset system	Ongoing	Monitoring of assets, equipment purchase, repair, allocation	IT Department
Access Rights	ISMS11 Access Control Policy, ISMS04 Information Security Policy ISMS07 Mobile Device and remote working Policy, HR24 Home- working Policy – Information Classification & Access Levels	Audit of systems, Opuz, Sage, Drive, user permissions	Yearly PPM	Audit of access provisioning & privileged access rights	IT Department

Additional information on change management can be found within IMS01.

Information Handling

Disposal of information

Any type of information must be disposed of securely. Confidential papers must be disposed of through confidential waste disposal companies approved by the company.

Following ISMS28 - Electronic information must be securely erased or otherwise rendered inaccessible prior to disposal of equipment.

Backups - Information owners must ensure that appropriate backup and system recovery measures are in place. Where backups are stored off site, appropriate

security measures must be taken to protect against unauthorised disclosure or loss. Recovery procedures should be tested on a regular basis.

Exchange of information
Whenever significant amounts of personal data or other confidential information are exchanged with other organisations, appropriate information security measures must be established to ensure the integrity and confidentiality of the data transferred. Regular exchanges must be covered by a formal written agreement with the third party.

When exchanging information by email or any other communication, recipient addresses should be checked carefully prior to transmission. Emails, telephone calls or any other communication requesting information which is not classified as public should not be acted upon until and unless the authenticity and validity of the communication has been verified.

Compliance

Noncompliance can lead to the loss of confidentiality, integrity and availability of information security systems and may result in criminal or civil actions against SMS Environmental Ltd. The loss or breach of confidentiality of contractually assured information may result in the loss of business, financial penalties or legal actions against SMS Environmental.