Information Security Policy

DOCUMENT CLASSIFICATION	Public
DOCUMENT REF	ISMS-DOC-05-4
VERSION	2
DATED	04 March 2022
DOCUMENT AUTHOR	Frankie Gallop
DOCUMENT OWNER	Adam Goldsmith

Socitm Advisory & Socitm

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
0.1	04/03/2022	Frankie Gallop	Initial draft
0.2	04/03/2022	Frankie Gallop	Needs reviewing
1	03/07/2022	Frankie Gallop	Final draft
2	03/11/2022	Frankie Gallop	Review of document

Distribution

NAME	TITLE

Approval

NAME	POSITION	SIGNATURE	DATE

Contents

Tables

1 Introduction

This document defines the information security policy of Socitm.

As a modern, forward-looking business, Socitm recognises at senior levels the need to ensure that its business operates smoothly and without interruption for the benefit of its customers, shareholders and other stakeholders.

In order to provide such a level of continuous operation, Socitm has implemented an Information Security Management System (ISMS) in line with the International Standard for Information Security, ISO/IEC 27001. This standard defines the requirements for an ISMS based on internationally recognised best practice.

The operation of the ISMS has many benefits for the business, including:

- Protection of revenue streams and company profitability
- Ensuring the supply of goods and services to customers
- Maintenance and enhancement of shareholder value
- Compliance with legal and regulatory requirements

Socitm has decided to maintain full certification to ISO/IEC 27001 in order that the effective adoption of information security best practice may be validated by an independent third party, a Registered Certification Body (RCB).

This policy applies to all systems, people and processes that constitute the organisation's information systems, including board members, directors, employees, suppliers and other third parties who have access to Socitm systems.

2 Information security policy

2.1 Information security requirements

A clear definition of the requirements for information security within Socitm will be agreed and maintained with the internal business so that all ISMS activity is focussed on the fulfilment of those requirements. Statutory, regulatory and contractual requirements will also be documented and input to the planning process. Specific requirements about the security of new or changed systems or services will be captured as part of the design stage of each project.

It is a fundamental principle of the Socitm Information Security Management System that the controls implemented are driven by business needs and this will be regularly communicated to all staff through team meetings and briefing documents.

Information security is all about keeping corporate information safe. The Policies address the need to protect confidential and sensitive information from disclosure, unauthorised access, loss, corruption and interference, and are relevant to information in both electronic and physical formats. Security can be defined by three things:-

- **Confidentiality** - information must not be made available or disclosed to unauthorised individuals, entities, or processes
- **Integrity** - data must not be altered or destroyed in an unauthorised manner, and accuracy and consistency must be preserved regardless of changes
- **Availability** - information must be accessible and useable on demand by authorised entities

A holistic approach to security encompasses the following areas:

- personnel security
- physical security
- communications security
- information security
- computer security
- technical security

2.2 Framework for setting objectives

A regular cycle will be used for the setting of objectives for information security, to coincide with the budget planning cycle. This will ensure that adequate funding is obtained for the improvement activities identified. These objectives will be based upon a clear understanding of the business requirements, informed by the management review process during which the views of relevant interested parties may be obtained.

Information security objectives will be documented for an agreed time period, together with details of how they will be achieved. These will be evaluated and monitored as part of

management reviews to ensure that they remain valid. If amendments are required, these will be managed through the change management process.

In accordance with ISO/IEC 27001 the reference controls detailed in Annex A of the standard will be adopted where appropriate by Socitm. These will be reviewed on a regular basis in the light of the outcome from risk assessments and in line with information security risk treatment plans. For details of which Annex A controls have been implemented and which have been excluded please see the *Statement of Applicability*.

In addition, enhanced and additional controls from the following codes of practice will be adopted and implemented where appropriate:

- ISO/IEC 27002 – Code of practice for information security controls

The adoption of these codes of practice will provide additional assurance to our customers and help further with our compliance with international data protection legislation.

2.3 Continual improvement of the ISMS

Socitm policy regarding continual improvement is to:

- Continually improve the effectiveness of the ISMS
- Enhance current processes to bring them into line with good practice as defined within ISO/IEC 27001 and related standards
- Achieve ISO/IEC 27001 certification and maintain it on an on-going basis
- Increase the level of proactivity (and the stakeholder perception of proactivity) with regard to information security
- Make information security processes and controls more measurable in order to provide a sound basis for informed decisions
- Review relevant metrics on an annual basis to assess whether it is appropriate to change them, based on collected historical data
- Obtain ideas for improvement via regular meetings and other forms of communication with interested parties
- Review ideas for improvement at regular management meetings in order to prioritise and assess timescales and benefits

Ideas for improvements may be obtained from any source including employees, customers, suppliers, IT staff, risk assessments and service reports. Once identified they will be recorded and evaluated as part of management reviews.

2.4 Information security policy areas

Socitm defines policy in a wide variety of information security-related areas which are described in detail in a comprehensive set of policy documentation that accompanies this overarching information security policy.

Each of these policies is defined and agreed by one or more people with competence in the relevant area and, once formally approved, is communicated to an appropriate audience, both within and external to, the organisation.

The table below shows the individual policies within the documentation set and summarises each policy's content and the target audience of interested parties.

POLICY TITLE	AREAS ADDRESSED	TARGET AUDIENCE
Internet Acceptable Use Policy	Business use of the Internet, personal use of the Internet, Internet account management, security and monitoring and prohibited uses of the Internet service.	Users of the Internet service
Mobile Device Policy	Care and security of mobile devices such as laptops, tablets and smartphones, whether provided by the organisation for business use.	Users of company-provided mobile devices
BYOD Policy	Bring Your Own Device (BYOD) considerations where personnel wish to make use of their own mobile devices to access corporate information.	Users of personal devices for restricted business use
Access Control Policy	User registration and deregistration, provision of access rights, external access, access reviews, password policy, user responsibilities and system and application access control.	Employees involved in setting up and managing access control
Cryptographic Policy	Risk assessment, technique selection, deployment, testing and review of cryptography, and key management	Employees involved in setting up and managing the use of cryptographic technology and techniques
Physical Security Policy	Secure areas, paper and equipment security and equipment lifecycle management	All employees
Information Security Policy for Supplier Relationships	Due diligence, supplier agreements, monitoring and review of services, changes, disputes and end of contract.	Employees involved in setting up and managing supplier relationships
Records Retention and Protection Policy	Retention period for specific record types, use of cryptography, media selection, record retrieval, destruction and review.	Employees responsible for creation and management of records
Privacy and Personal Data Protection Policy	Applicable data protection legislation, definitions and requirements.	Employees responsible for designing and managing systems using personal data
HR Security Policy	Recruitment, employment contracts, policy compliance, disciplinary process, termination	All employees
Acceptable Use Policy	Employee commitment to organisational information security policies.	All employees

Table 1: Set of policy documents

2.5 Application of information security policy

The policy statements made in this document and in the set of supporting policies listed in Table 1 have been reviewed and approved by the top management of Socitm and must be complied with. Failure by an employee to comply with these policies may result in disciplinary action being taken in accordance with the organisation's *Employee Disciplinary Process*.

Questions regarding any Socitm policy should be addressed in the first instance to the employee's immediate line manager.

3 Socitm's Obligations:

The Operations Board shares the responsibility for information security to ensure that:

- The Socitm's Policies, Guidelines and Procedures are approved, published, communicated, reviewed and continue to meet business needs
- That any significant change in the exposure of information to security threats is identified and managed
- All security incidents are monitored and reviewed
- Major initiatives to improve information security are approved and authorised
- Information security controls across the organisation are co-ordinated
- Responsibilities for the protection of information and information system assets are clearly defined and allocated
- The appropriate structure is implemented to effectively manage information security
- Procedural documentation to support Policy requirements is developed and maintained
- The purpose, use and implementation of any new information processing mechanism, channel or facility is approved
- There is transparency in the decision-making process to ensure accountability
- Appropriate inter-organisation agreements relating to security requirements and common minimum standards are in place
- Advice is sought from qualified security specialists as and when required.
- Staff have the equipment and skills to perform their duties in accordance with the Socitm's Policies
- Staff are aware of their obligations with regard to IT security.

Signed by:

Adam Goldsmith

Approved by:

Socitm Management