Socitm

Information Security Policy

17th November 2025

Contents

Tables

Introduction

This document defines the information security policy of Socitm.

As a modern, forward-looking charity, Socitm recognises at senior levels the need to ensure that its business operates smoothly and without interruption for the benefit of its members stakeholders. To this end, Socitm are committed to attain and retain Cyber Essentials + accreditation.

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.

Information security policy

Information security requirements

A clear definition of the requirements for information security within Socitm will be agreed and maintained with the internal business. 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

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 policy areas

Socitm defines policy in a wide variety of information security-related areas which are described in the staff handbook.

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
IT and Communications Systems Policy	Device security & passwords. Systems & data security. Email, messaging systems and use of the Internet (both business & personal)	All employees & trustees.
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

Table 1: Set of policy documents

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.

Socitm’s Obligations:

The Executive Management Team shares the responsibility for information security to ensure that:

- 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
- 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:

David Bryant

Approved by:

Socitm Management