Swiftbon

Information Security Policy

Document Classification:	Internal
Document Ref.	SWIFTBON-ISMS-DOC-Information Security Policy
Version:	1.0
Dated:	15th June 2025
Document Owner:	Information Security Officer

Revision History

Version	Date	Revision Author	Summary of Changes
1.0	15 of June 2025	Information Security Officer	Initial Content Creation

Approval

Name	Position	Signature	Date
	CISO		20-August-2025
	CEO/CTO		24-August-2025

Contents

List of Tables

1. Introduction

This document defines the information security policy of Swiftbon Limited. As a modern, forward-looking business, Swiftbon Limited 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, Swiftbon Limited 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 recognized best practices.

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

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

Swiftbon Limited 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) at the point of this policy taking effect or in the future.

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

The scope or impact is any access, logical or physical, that has the potential to affect Swiftbon Limited platforms negatively. Areas that are managed include, but are not limited to

Physical Security	**Logical Security**
Network security and monitoring	Application security
Segregation of duties	Establishing, editing, and terminating user access
Backup and recovery	Business continuity
Incident Response	Third-party security
Security education and awareness	Data storage
Handling and distribution of data	Confidential information
Password policies	Security monitoring
Access to customer data	Threat reporting and response

2. Information Security Policy

2.1 Information Security Requirements

A clear definition of the requirements for information security within Swiftbon Limited will be agreed and maintained with the internal business so that all ISMS activity is focused on the fulfillment of those requirements. Statutory, regulatory, and contractual requirements will also be documented and input into the planning process. Specific requirements regarding 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 Swiftbon Limited 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.

2.2 Information Security Policy Areas

Swiftbon Limited 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 organization.

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**
Mobile Device Policy	Care and security of mobile devices such as laptops, tablets, and smartphones, whether provided by the organization or the individual for business use.	Users of company-provided and BYOD (Bring Your Own Device) mobile devices
Teleworking Policy	Information security considerations in establishing and running a teleworking site and arrangement e.g. physical security, insurance, and equipment	Management and employees involved in setting up and maintaining a teleworking site
Cloud Computing Policy	This policy addressed Infrastructure as a service - IAAS, Software as a service - SAAS, Platform as a service -PAAS, Cloud storage, back up and disaster recovery.	This applies to IT/Engineering and users of cloud services within the Organisation
Asset Management Policy	Assets within Swiftbon Limited are tracked with respect to its criticality to both owners and users and to allow for easy tracking of assets	All employees within the Organisation
Acceptable use policy	Network and protection of sensitive information, client data, and usage of all identified assets are addressed with due diligence and disciplinary action should a breach happens	All employees within the Organisation
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/Monitoring Policy	Secure areas, paper, and equipment security, and equipment lifecycle management	All employees
Anti-Malware Policy	Firewalls, anti-virus, spam filtering, software installation and scanning, vulnerability management, user awareness training, threat monitoring and alerts, technical reviews, and malware incident management.	Employees responsible for protecting the organization’s infrastructure from malware
Backup Policy	Backup cycles, cloud backups, off-site storage, documentation, recovery testing, and protection of storage media	Employees responsible for designing and implementing backup regimes

Software Policy	Purchasing software, software registration, installation and removal, in-house software development, and use of software in the cloud.	All employees
Technical Vulnerability Management Policy	Vulnerability definition, sources of information, patches and updates, vulnerability assessment, hardening, and awareness training.	Employees responsible for protecting the organization’s infrastructure from malware
Network Security Policy	Network security design, including network segregation, perimeter security, wireless networks, and remote access; network security management, including roles and responsibilities, logging and monitoring, and changes.	Employees responsible for designing, implementing, and managing networks
Electronic Messaging Policy	Sending and receiving electronic messages, monitoring of electronic messaging facilities, and use of email.	Users of electronic messaging facilities
Secure Development Policy	Business requirements specification, system design, development, testing, and outsourced software development.	Employees responsible for designing, managing, and writing code for bespoke software developments
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
Business Continuity and Availability Management Policy	Availability requirements and design, monitoring and reporting, non-availability, testing availability plans, and managing changes.	Employees responsible for designing systems and managing service delivery
IP and Copyright Compliance Policy	Protection of intellectual property, the law, penalties, and software license compliance.	All employees
Records/Data Retention and Protection Policy	Retention period for specific record types, use of cryptography, media selection, record retrieval, destruction, and review.	Employees responsible for the creation and management of records
Clear Desk and Clear Screen Policy	Security of information shown on screens printed out and held on removable media.	All employees
Privacy and Personal Data Protection Policy	Costumers and employee's data are protected in line with relevant legislation and steps taken to comply with it	All employees
Threat intelligence Policy		All employees
Configuration Management Policy		All employees

Table 1 - Set of policy document

2.3 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 Swiftbon Limited 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 organization's *Employee Disciplinary Process.*

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