www.f-si.co.za

FSI

INFORMATION SECURITY POLICY

FSI.PO.05

Document Owner: Operations Director
Document Version: 02
Creation Date: October 2023
Last Review Date: January 2025

Table of Contents

1. Document Control

1.1. Version Control

Document Name	Information Security Policy
Document No. and Version	FSI.PO.05 Version 2
Next Review Date	January 2027
Date Last Reviewed	January 2025
Authors	Operations Director

1.2. Updates to this document

This document will be reviewed biennially, or when changes to legislation and control processes or procedures occur.

1.3. Change History

All changes to this document must be approved and authorised by the Operations Director.

The record below is to be completed by the person making the amendment(s). Each new document will have a version number and date of issue printed on it. If a review is performed, and no changes to the document is made, the issue date will be updated, but not the version number. Format changes do not require a new version number or issue date.

Version	Issue Date	Pages Amended	Amended by	Approved by
1.0	15/11/2023	All – Policy Created	J. Stols	P. Pather
2.0	Jan 2025	Updated the policy approvers.	J. Stols	S. Hayes

1.4. Distribution

Once approved, the document will be circulated to the following individuals:

Issued To	Issue Date	Position/s
All FSI Employees	15/01/2024	All
All FSI Employees	20/02/2025	All

The Information Security Policy document is available to all FSI employees on the company shared drive.

2. Purpose

FSI recognises the critical importance of safeguarding information assets from unauthorised access, disclosure, alteration, and destruction. This Information Security Policy outlines the principles and guidelines that govern the protection of information to ensure the confidentiality, integrity, and availability of data. FSI has implemented an Information Security Management System that complies with the requirements of ISO27001:2022 and its supporting standards to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

3. Scope

This Information Security Policy applies to all FSI Management in terms of their roles and responsibilities in securing information, implementing, maintaining, and continuously improving the FSI ISMS. It also assures our clients whose information we process, that adequate and effective controls have been implemented to safeguard their information.

4. Policy Requirements

4.1. Management Commitment

FSI's directors are committed to the protection of information and associated assets, whether owned or managed by FSI. In line with our business strategy to be an international thought leader in information security services and the requirements defined by interested stakeholders, we have implemented an ISMS to manage and protect information in accordance with internationally recognised standards. As the leaders of FSI, we are committed to the following:

4.1.1. Establish, implement and maintain an information security management system that complies with the requirements of ISO 27001:2022.

4.1.2. Satisfy applicable requirements related to information security.

4.1.3. Identify, analyse and evaluate information security risks and apply a risk treatment process with adequate controls.

4.1.4. Establish information security objectives that are compatible with the strategic direction of the organisation.

4.1.5. Ensuring the availability of resources needed for the effective implementation, maintenance and continual improvement of the information security management system.

4.1.6. Assigning roles and responsibilities for information security.

4.1.7. Communicating the importance of effective information security management and conforming to the information security management system requirements.

4.1.8. Ensuring that the information security management system achieves its intended outcomes;

4.1.9. Comply with applicable information security legislation, regulations, and other requirements and, where appropriate, proactively seek to meet future legislative requirements cost-effectively.

4.1.10. Directing and supporting persons to contribute to the effectiveness of the information security management system.

4.1.11. Supporting management roles to demonstrate their leadership as it applies to their areas of responsibility.

4.1.12. Ensuring this policy, and its contents, are available to all stakeholders.

4.1.13. Improve information security awareness through training, development and education.

4.1.14. Periodically undertake audits of the information security management systems to enhance information security performance.

4.1.15. Continually improving the FSI information security management system.

4.2. Information Security Objectives

4.2.1. FSI's Information Security Objectives are crucial to the ISMS and our strategic direction for protecting information assets. Our framework for setting information security objectives is as follows:

4.2.1.1. Information security risks are understood and treated to be acceptable to the organisation.

4.2.1.2. The confidentiality of client information, information processed when performing services, and all service delivery reports are protected.

4.2.1.3. The confidentiality of employee information is protected.

4.2.1.4. Compliance with applicable legislation and regulations is ensured.

4.2.1.5. The integrity of accounting records is preserved.

4.2.1.6. Company networks and devices are protected from unauthorised access.

4.3. Roles and Responsibilities for Information Security

4.3.1. The nature of FSI's business is information security, and therefore all employees are essentially familiar with information security and the services that we provide to assist our clients with the protection of their information and associated assets.

4.3.2. FSI have appointed an Information Security Committee that is responsible for directing, monitoring, implementing and improving the FSI ISMS. The FSI Operations Director is the committee chair.

4.3.3. FSI Directors are responsible for ensuring that all employees:

4.3.3.1. are properly briefed on their information security roles and responsibilities before being granted access to the organisation's information and other associated assets;

4.3.3.2. are provided with guidelines which state the information security expectations of their role within the organisation;

4.3.3.3. are mandated to fulfil the information security policy and topic-specific policies of the organisation;

4.3.3.4. achieve a level of awareness of information security relevant to their roles and responsibilities within the organisation;

4.3.3.5. compliance with the terms and conditions of employment, contract or agreement, including appropriate methods of working;

4.3.3.6. continue to have the appropriate information security skills and qualifications through ongoing professional education;

4.3.3.7. are provided with adequate resources and project planning time for implementing the organisation's security-related processes and controls.

4.4. Information Security Principles

4.4.1. Information risks are understood, monitored and treated when necessary.

4.4.2. All staff are made aware and accountable for information security as relevant to their role.

4.4.3. Provision is made for funding information security controls in operational and project management processes.

4.4.4. Possibilities for fraud associated with abuse of information systems is taken into account in the overall management of information systems.

4.4.5. Information security status reports are available.

4.4.6. Information security risks are monitored and action is taken when changes result in risks that are not acceptable.

4.4.7. Situations that could place FSI in breach of laws and statutory regulations will not be tolerated.

4.5. Information Security Management System

4.5.1. FSI's ISMS follows a risk-based approach with people, processes and technological controls to mitigate any potential risks.

4.5.2. Information security policies, procedures and standards have been defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties,

4.5.3. The FSI ISMS undergoes independent reviews of people, processes and technologies to ensure the continuing suitability, adequacy and effectiveness of the information security controls.

5. Breaches of this Policy

Breaches of this policy will be handled in accordance with FSI's performance management and disciplinary procedures.

6. Policy Approval

Authorised by:	Director: J. Stols		20/02/2025
		Signature	Date
	Director: S. Hayes		20/02/2025
		Signature	Date

7. Roles and Responsibilities

Role	Responsibility
Document Owner	Review and update this policy when required.
COO	Provide approvals for any exceptions to this policy.
FSI Directors	Comply with policy requirements.

8. References

- ISO27001:2022 Information: Information security, cybersecurity, and privacy protection — Information security management systems — Requirements.
- ISO27002:2022 Information security, cybersecurity, and privacy protection — Information security controls.
- Protection of Personal Information Act, 4 of 2013.
- FSI.PO.06 Privacy Polic
- FSI.PO.07 Third Party Policy
- FSI.PO.08 End-User Computing Policy
- FSI.PO.09 ICT Security Policy

9. Policy Definitions

Term	Definition
Information Security	Information security, often abbreviated as "infosec," is the practice of protecting information by mitigating information risks. It encompasses measures, processes, and technologies that are designed to ensure the confidentiality, integrity, and availability of data and information systems.
Confidentiality	Information security ensures that sensitive data is not disclosed to unauthorised individuals or entities. This involves controlling access to information and preventing data breaches or leaks.

Integrity	Information integrity ensures that data remains accurate, consistent, and unaltered. It involves protecting data from unauthorised modifications, whether intentional or accidental.
Availability	Information security also focuses on making sure that data and information systems are accessible and available when needed. This includes preventing disruptions, downtime, and denial of service attacks.

FSI

Get In Touch

FSI (PTY)LTD
Ground Floor Block D
55 Kyalami Boulevard
Kyalami Business Park
Gauteng
1683

www.f-si.co.za

@FSI – Forensic Sciences Institute