SIMUNIX

Simunix ISMS Executive Summary v1.1

JOHN LAWRENCE LEWIS

Document Information

Reference	ISO 27001
Category	Information Security Management System (ISMS) Documents
Title	ISMS Executive Summary
Author	John Lawrence Lewis
Compliance	ISO 27001:2022
Review Plan	Annually
Next Review Date	August 2025
Related Documents	Simunix ISMS Mandatory Clauses

Version History

Version	Date	Author	Description of change
1.0	10/01/2024	John Lawrence Lewis	Published version
1.1	01/08/2024	John Lawrence Lewis	Annual review, no revision

Contents

1.0 Policy Statement

At Simunix we are committed to protecting the confidentiality, integrity, and availability of our information assets. Information security is a critical aspect of our business operations, and we recognise its importance in safeguarding our data, our clients' data, and maintaining the trust of our stakeholders.

1.1 Purpose

This ISMS Policy establishes a framework for managing and continuously improving information security within our organisation. Our primary objectives are to:

- Protect sensitive information from unauthorised access, disclosure, alteration, or destruction.
- Comply with applicable laws, regulations, and industry standards related to information security.
- Mitigate information security risks that may impact our business operations.

1.2 Scope

This policy applies to all employees, contractors, suppliers, and third parties who have access to our information assets and systems. It covers all information assets owned, managed, or processed by Simunix.

1.3 Objectives

Our key objectives for information security include:

- Ensuring the confidentiality of sensitive data, including client information and intellectual property.
- Maintaining the integrity and accuracy of data and systems.
- Ensuring the availability and reliability of critical business systems.
- Promoting a culture of information security awareness and responsibility among all stakeholders.

1.4 Roles and Responsibilities

All employees are responsible for complying with information security policies and reporting security incidents.

The IT Director and DPO are accountable for overseeing the ISMS and ensuring its effectiveness.

1.5 Legal and Regulatory Compliance

We are committed to complying with all relevant laws and regulations related to information security, data protection, and privacy.

1.6 Risk Management

We will regularly assess information security risks and implement appropriate controls to mitigate these risks.

1.7 Security Controls

We will implement necessary security controls and safeguards to protect our information assets, including access controls, encryption, and regular security updates.

1.8 Incident Reporting and Response

We have established procedures for reporting and responding to information security incidents promptly.

1.9 Training and Awareness

We will provide information security training and awareness programs for employees to ensure they understand their roles and responsibilities in maintaining information security.

1.10 Review and Audit

We will periodically review and audit our ISMS to assess its effectiveness and compliance with this policy.

1.11 Communication

This ISMS Policy will be communicated to all employees during onboarding and made readily available through our company intranet. Updates and changes will also be communicated as necessary.

1.12 Enforcement and Consequences

Non-compliance with this policy may result in disciplinary actions, up to and including termination of employment or contractual relationships.

1.13 Review and Revision

This ISMS Policy will be reviewed and updated as needed to reflect changes in our business, technology, or regulatory requirements.

1.14 Policy communication

At Simunix our ISMS Policy is a document that guides our commitment to information security. To ensure that our policy is effectively communicated we have implemented the following processes:

1. **Employee Orientation**: During the onboarding process, all new employees will receive a copy of the ISMS Policy and be provided with an overview of its importance and relevance to their roles.
2. **SharePoint**: The complete ISMS Policy document is accessible on our company SharePoint site, where employees can review it at any time.
3. **Training and Awareness Programs**: We conduct periodic information security training sessions to reinforce the principles outlined in the ISMS Policy and raise awareness among our team.
4. **Email Notifications**: Important updates or changes to the ISMS Policy will be communicated to all employees via email.
5. **Leadership Support**: Company leadership will actively support and endorse the ISMS Policy, emphasising its significance within the organisation.
6. **Feedback Mechanism**: We encourage employees to provide feedback or seek clarifications related to the ISMS Policy through designated channels.
7. **Continuous Improvement**: We are committed to continuously improving our information security practices in line with the ISMS Policy's objectives.

This policy is essential in ensuring that we protect sensitive information, comply with legal and regulatory requirements, and maintain trust with our clients and stakeholders.

1.15 Approval

This scope statement has been reviewed and approved by John L Lewis, Simunix DPO.