INFORMATION SECURITY MANAGEMENT SYSTEM

ISMS Policy

Signed

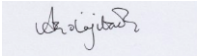
Name	Position	Signature	Date
Adeola Ajibade	Managing Director		19/01/2026

Table of Contents

1. Introduction

This policy defines how the Information Security Management System ("ISMS") will be set up, managed, measured, reported on, and developed within FactoreX.

FactoreX is committed to providing a service according to client's expectations, ensuring that we take all aspects of Information Security in delivering our services to our clients.

It is the policy of FactoreX to commit and maintain an information security management system designed to meet the requirements of ISO 27001:2022 in pursuit of its primary objectives.

To drive continual improvement within the information security management system, FactoreX has set objectives on an annual basis as part of the Management Review Process; these objectives ensure the system is appropriately monitored and measured. All objectives are communicated to all staff and include key responsibilities, timescales, and appropriate measures of success.

It is our policy to ensure that

- All information and systems will be protected against unauthorized access and disclosure.
- Confidentiality of information will be maintained.
- Integrity of information is protected from unauthorized modification.
- Regulatory and legislative requirements will be met.
- Business continuity plans will be maintained and tested (as far as practicable)
- All suspected breaches of information security will be reported and investigated.
- Adequate prevention and detection of malware is in place.
- Information Security Policies are in place to ensure the safe practice of using our computer and information systems.
- Quality products and services are always rendered to customers.
- Customers' needs and expectations are met In line with the agreed service and requirements.
- Competent external providers that meet all pre-qualifications requirements are engaged.
- Optimal internal business processes and customer satisfaction, delight, and retainership.
- Continually improve the effectiveness of the Service Management System and services

2. ISMS Policy Statements

"FactoreX is committed to maintaining and improving its information security by implementing and maintaining an Information Security Management System based on ISO 27001:2022. Factorex aims to meet and exceed the expectations of its stakeholders, comply with all relevant regulations and industry requirements."

3. Setting the ISMS Objectives

The high-level objectives for the ISMS within FactoreX are defined within the document ISMS Context, Requirements and Scope. These are fundamental to the nature of the business and are not subject to frequent change.

These overall objectives will be used as guidance in the setting of lower level, more short-term objectives for planning within an annual cycle timed to coincide with organisational budget planning.

This will ensure that adequate funding is obtained for the improvement activities identified. These objectives will be based upon a clear understanding of the overall business requirements and how they may change during the year.

4. Top Management Leadership and Commitment

Commitment to the information security management system objectives extends to senior levels of the organization and will be demonstrated through this ISMS Policy and the provision of appropriate resources to provide and develop the ISMS and associated controls.

Top management will also ensure that a systematic review of the performance of the programme is conducted on a regular basis to ensure that the objectives are being met, and relevant issues are identified through the audit programme and management review processes. Management review can take several forms including departmental and other management meetings.

The top management shall have overall authority and responsibility for the implementation and management of the information security management system, specifically:

- The identification, documentation and fulfilment of the information security management system objectives.
- Implementation, management, and improvement of risk management processes
- Integration of operational processes, procedures, and controls
- Compliance with statutory, regulatory, and contractual requirements
- Reporting to top management on performance and improvement

4.1 Commitment to Satisfying Applicable Requirements

Commitment to the delivery of ISMS extends to senior levels of the organization and will be demonstrated through this Information Security Management System Policy and the provision of appropriate resources to establish and develop the ISMS.

Top management will also ensure that a systematic review of the performance of the programme is conducted on a regular basis to ensure that ISMS objectives are met, and information security issues are identified through the audit programme and management processes. Within the field of information security management system, there are several key roles that need to be undertaken to ensure the success of the ISMS and protect the business from risk.

FactoreX Top Management is also committed to satisfying the following applicable requirements with regards to the ISMS by:

- Ensuring improvement of the ISMS
- Providing necessary human, financial and technological resources to establish and develop information security management systems
- Providing direction and support for information security in accordance with business requirements and relevant laws and regulations
- Establishing a management framework to initiate and control the implementation and operation of information security within the organization
- Ensuring that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered
- Ensuring that information receives an appropriate level of protection in accordance with its importance to the organization
- Ensuring authorized user access and prevent unauthorized access to systems and services
- Making users accountable for safeguarding their authentication information
- Limiting access to information and information processing facilities
- Ensuring proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information in Factorex
- Preventing unauthorized physical access, damage and interference to the organization's information and information processing facilities
- Ensuring correct and secure operations of information processing facilities
- Ensuring the protection of information in networks and supporting information processing facilities using technologies
- Ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks
- Ensuring the operation of the service management system in the organization
- Operating the ISMS, ensuring coordination of the activities and the resources
- Ensuring Control of parties involved in the service lifecycle
- Ensuring business relationship management and agreement between parties involved in the service lifecycle

- Budgeting and accounting for services or groups of services in accordance with its financial management policies and processes

5. Continual Improvement of the ISMS

FactoreX policy regarding continual improvement are to:

- Continually improve the effectiveness of the ISMS
- Enhance current processes to bring them into line with good practice as defined within ISO/IEC 27001:2022
- Achieve Certification and maintain it on an on-going basis
- 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, including cloud service customers
- Review ideas for improvement at regular management meetings 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.

6. Governance of Information Security

6.1. Principles Guiding Information Security Activities

All information security activities within FactoreX are governed by the following principles:

- **Confidentiality**: Ensuring that sensitive information are accessible only to those authorized to have access.
- **Integrity**: Maintaining the accuracy, completeness, and trustworthiness of data throughout its lifecycle.
- **Availability**: Ensuring that authorized users have reliable and timely access to required information and systems.
- **Risk-Based Approach**: Prioritizing security controls and resources based on identified risks to sensitive data and business operations.
- **Least Privilege**: Limiting access rights for users to the minimum necessary to perform their job responsibilities.
- **Compliance**: Adhering to all applicable legal, regulatory, and contractual requirements.
- **Continuous Improvement**: Proactively reviewing and enhancing information security processes and technologies in response to emerging threats and business changes.

These principles apply to all staff, contractors, and service providers who interact with the FactoreX system.

6.2. Assignment of Responsibilities for Information Security

The organization ensures that specific roles and responsibilities for information security are clearly defined and assigned as follows:

- **Executive Management**: Provides strategic direction, approves information security policies, and ensures necessary resources are allocated.
- **IT Operations Team**: Implements technical controls, conducts system monitoring, and supports incident response activities.
- **Compliance Team**: Monitors regulatory compliance, coordinates audits, and tracks remediation efforts.
- **Managers**: Ensure implementation of security controls within their respective domains and promote staff awareness.
- **All Employees**: Responsible for understanding and complying with security policies and promptly reporting any suspicious activity or incidents.
- Role-based accountability ensures that information security is integrated into the daily activities of all departments.

6.3. Procedures for Handling Exemptions and Exceptions

From time to time, operational needs may necessitate temporary or permanent exemptions from specific information security controls or policies. The following procedure governs such cases:

1. **Formal Request**: A request for exemption or exception must be submitted in writing to the ISMS Manager, clearly stating:
    - The control or requirement to be exempted from,
    - The business justification,
    - Duration of the exemption,
    - Proposed alternative controls (if any).

2. **Risk Assessment**: The ISO, in collaboration with the Compliance Team, shall evaluate the request based on its impact on confidentiality, integrity, and availability of systems and data.

3. **Approval Process**: Exceptions can only be granted with documented approval from Executive Management. Where applicable, the decision must consider compliance implications (e.g., ISMS requirements).

4. **Documentation and Review**: All approved exceptions shall be recorded, periodically reviewed, and either renewed or revoked based on changes in business or risk environment.

By managing exceptions systematically, FactoreX ensures that business agility does not compromise overall security or compliance integrity.