					Insert Registered Legal Entity Name Here							
Document number: P01					Document Title: **Information Security Policy**							
Version: 1.0		Effective Date: 01.01.2025			Document Owner:							
X	Policy		Standard		Procedure		Form		Register		Other	

Revision history				
Revision number	**Revision Date**	**Changes**	**Reviewed by**	**Process owner**

Approvals			
Name	**Title**	**Date**	**Signature**

1. Purpose

1.1 This policy defines the organization's overarching commitment to information security through the establishment of a formal Information Security Management System (ISMS).

1.2 It provides the strategic direction and foundational requirements for protecting the confidentiality, integrity, availability, and resilience of all information assets across physical, digital, and cloud environments.

1.3 This policy fulfills ISO/IEC 27001:2022 Clauses 5.1 and 5.2 by expressing leadership intent, Top Management commitment, and alignment of security activities with organizational objectives.

1.4 It serves as the authoritative reference for all subordinate policies, standards, and procedures within the ISMS and is essential to enabling a risk-based, compliance-driven, and continually improving security environment.

2. Scope

2.1 This policy applies to all individuals, assets, and processes defined within the ISMS scope, including:

2.1.1 All business units, departments, subsidiaries, and branches

2.1.2 Employees, contractors, temporary staff, consultants, and third-party service providers

2.1.3 All data, information systems, applications, IT infrastructure, and communications systems

2.1.4 All physical, cloud-based, remote, and hybrid environments where company data is processed or accessed

2.2 This policy is binding on all entities handling organizational information and applies to all stages of the information asset lifecycle, from creation and transmission through storage and disposal.

2.3 Any exclusions or limitations to this scope shall be documented in the ISMS Scope Statement and justified with formal approval from Top Management.

3. Objectives

3.1 To establish an ISMS that is aligned with ISO/IEC 27001:2022 and capable of supporting risk-based decision-making across the enterprise.

3.2 To ensure the principles of confidentiality, integrity, and availability are embedded in all organizational activities, systems, and partnerships.

3.3 To enable regulatory and contractual compliance by defining measurable objectives and integrating them into business operations.

3.4 To minimize the likelihood and impact of information security incidents through effective preventive, detective, and corrective controls.

3.5 To drive continual improvement in information security maturity through defined performance indicators, audit results, and ISMS management reviews.

3.6 To promote a culture of accountability, awareness, and resilience in which security responsibilities are understood and fulfilled by all personnel.

4. Roles and Responsibilities

4.1 Top Management

4.1.1 Approves and endorses this Information Security Policy and the implementation of the ISMS framework.

4.1.2 Ensures alignment between security objectives and business strategy.

4.1.3 Leads by example and promotes a strong information security culture.

4.1.4 Reviews and approves major changes to ISMS scope, risk treatment, and governance structure.

4.2 Chief Information Security Officer (CISO) / ISMS Manager

4.2.1 Owns the ISMS and maintains this policy in compliance with ISO/IEC 27001.

4.2.2 Leads risk assessments, control implementation, and continual improvement activities.

4.2.3 Ensures cross-functional coordination of security efforts and oversees subordinate policies.

4.2.4 Reports ISMS status, incidents, audit results, and metrics to Top Management.

4.2.5 Ensures policy reviews and updates are conducted in accordance with Section 9 of this document.

[... Sections 4.3–8 are not included in this preview. Purchase the full document to access the complete policy content. ...]

9. Review and Update Requirements

9.1 Review Frequency

9.1.1 This policy shall be reviewed at least annually or upon any of the following triggers:

9.1.1.1 Significant changes to legal, regulatory, or contractual obligations

9.1.1.2 Material changes to the organizational risk profile

9.1.1.3 Results of internal or external audits

9.1.1.4 Major incidents or control failures

9.2 Review Authority and Process

9.2.1 The CISO or designated ISMS Manager shall lead the review process.

9.2.2 Inputs to the review shall include:

9.2.2.1 Internal audit results

9.2.2.2 Risk assessment trends

9.2.2.3 Changes to business processes and technology

9.2.2.4 Performance against KPIs and risk thresholds

9.2.3 All updates shall:

9.2.3.1 Be version-controlled and documented

9.2.3.2 Be approved by Top Management

9.2.3.3 Be communicated to all affected parties through official communication channels

9.2.3.4 Trigger necessary updates to subordinate documentation and training

10. Related Policies and Linkages

10.1 This foundational policy is directly linked to the following organizational security policies and frameworks:

10.1.1 P2 – Governance Roles & Responsibilities Policy: Defines the governance structure and authority hierarchy referenced in this document.

10.1.2 P3 – Acceptable Use Policy (AUP): Establishes behavioral requirements and appropriate handling of information assets.

10.1.3 P4 – Access Control Policy: Operationalizes access-related controls derived from this overarching policy.

10.1.4 P6 – Risk Management Policy: Provides the risk-based context for selecting controls and accepting residual risk.

10.1.5 P33 – Audit and Compliance Monitoring Policy: Specifies how internal assurance mechanisms validate policy enforcement.

10.2 These interdependencies ensure comprehensive alignment and traceability across the ISMS and support unified risk and compliance governance.

11. Reference Standards and Frameworks

11.1 This Information Security Policy is formally aligned with the following standards and frameworks to ensure compliance, audit readiness, and regulatory defensibility:

11.2 ISO/IEC 27001

11.2.1 Clause 5.1 – Leadership and Commitment: This policy demonstrates Top Management's commitment to information security and defines responsibilities and resource allocations for the ISMS.

11.2.2 Clause 5.2 – Information Security Policy: This document serves as the organization's formal information security policy, aligned with stated security objectives, business strategy, and ISO/IEC 27001 compliance.

11.2.3 Clause 6.1 – Actions to Address Risks and Opportunities: The risk-based approach reflected in this policy ensures that security resources are applied proportionately to threats.

11.2.4 Clause 9.2 – Internal Audit and Clause 10 – Improvement: This policy is embedded in the organization's continual improvement lifecycle and is subject to internal audit validation.

11.2.5 ISO/IEC 27002:2022 – Control 5.1: Specifies guidance for establishing and maintaining information security policies. This policy reflects ISO/IEC 27002 recommendations for hierarchical documentation, review cycles, and enforceability.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 (Security Planning Policy and Procedures): This policy satisfies the requirement to develop, disseminate, and review a formal, organization-wide information security policy.

11.3.2 PM-1 through PM-5: Addresses program-level governance, including information security roles, resource allocation, risk strategy, and integration of security planning into enterprise operations.

11.4 EU GDPR (2016/679)

11.4.1 Article 5(2): Enforces the principle of accountability. This policy defines responsible parties and traceable enforcement actions.

11.4.2 Article 24: Requires implementation of technical and organizational measures, including policies aligned with risk.

11.4.3 Article 32: Supports implementation of appropriate measures to ensure the security of personal data throughout its lifecycle.

11.5 EU NIS2 Directive (2022/2555)

11.5.1 Article 21(2)(a): Requires entities to implement a documented security policy addressing risk management and governance. This policy meets that requirement and supports broader cybersecurity readiness and critical infrastructure protection.

11.6 EU DORA (2022/2554)

11.6.1 Article 5(2): Requires a documented internal control framework for ICT risk management. This policy supports financial sector compliance by assigning roles, controls, and oversight functions aligned with DORA governance expectations.

11.7 COBIT 2019

11.7.1 EDM01 – Governance Framework Setting: This policy supports enterprise governance by defining ISMS roles, leadership commitments, and strategic objectives.

11.7.2 APO01 – Management Framework: Supports the establishment and operation of a structured ISMS.

11.7.3 APO12 – Risk Management: Provides the foundation for information security risk governance.

11.7.4 MEA01/MEA03 – Monitor, Evaluate and Assess: Reinforces continuous performance evaluation and internal control monitoring through policy compliance enforcement.