					[Insert Registered Legal Entity Name Here]									
Document number: P1					Document Title: **Information Security Policy**									
Version: 1.0		Effective Date: 01.01.2025			Document Owner: IT									
X	Policy		Standard		Procedure		Form		Register		Other			

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

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

Aligned with standards and regulations where applicable		
Standard/Regulation	**Clause/Article**	**Comment**
ISO/IEC 27001:2022	Clauses 5.1, 5.2, 6.1, 9.2, 10	
ISO/IEC 27002:2022	Control 5.1	
NIST SP 800-53 Rev.5	PL-1, PM-1 through PM-5	
EU GDPR	Articles 5(2), 24, 32	
EU NIS2	Article 21(2)(a)	
EU DORA	Article 5(2)	
COBIT 2019	EDM01, APO01, APO12, MEA01/03	

					[Insert Registered Legal Entity Name Here]									
Document number: P1					Document Title: **Information Security Policy**									
Version: 1.0		Effective Date: 01.01.2025			Document Owner: IT									
X	Policy		Standard		Procedure		Form		Register		Other			

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 The policy fulfills ISO/IEC 27001:2022 Clause 5.2 and Clause 5.1 by expressing leadership intent, top management commitment, and alignment of security activities with organizational objectives.

1.4 It acts as the authoritative reference for all subordinate policies, standards, and procedures within the ISMS and is essential for 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 scope of the ISMS, 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, infrastructure, and communications channels

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

2.2 The policy is binding on all entities handling organizational information and applies to all stages of the information lifecycle—from creation and transmission to storage and disposal.

2.3 Any exclusions or limitations to this scope must be documented in the ISMS scope statement and justified with formal approval from executive management.

3. Objectives

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

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

3.3 To enable regulatory and contractual compliance by defining measurable, policy-driven security 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 outcomes, and management reviews.

3.6 To promote a culture of accountability, awareness, and resilience where security responsibilities are understood and executed by all personnel.

4. Roles and Responsibilities

4.1 **Executive Management**

4.1.1. Approves and endorses the Information Security Policy and 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.

[.....]

Reference Standards and Frameworks

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

ISO/IEC 27001:2022

- **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.
- **Clause 5.2 – Information Security Policy**: This document serves as the organization's formal security policy, aligned with stated security objectives, business strategy, and ISO/IEC 27001 compliance.
- **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.
- **Clause 9.2 – Internal Audit** and **Clause 10 – Improvement**: This policy is embedded in the organization's continual improvement lifecycle and subject to internal audit validation.
- **ISO/IEC 27002:2022 – Control 5.1** Specifies guidance for establishing and maintaining security policies. This policy mirrors ISO 27002 recommendations for hierarchical documentation, review cycles, and enforceability.

NIST SP 800-53 Rev.5

- **PL-1 (Security Planning Policy and Procedures)**: This policy satisfies the requirement to develop, disseminate, and review a formal, organization-wide information security policy.
- **PM-1 through PM-5**: Addresses program-level governance including information security roles, resource allocation, risk strategy, and security planning integration into enterprise operations.

EU GDPR (2016/679)

- **Article 5(2)**: Enforces the principle of accountability. This policy defines responsible parties and traceable enforcement actions.
- **Article 24**: Requires implementation of technical and organizational measures, including policies aligned with risk.
- **Article 32**: Supports implementation of appropriate measures to ensure security of personal data throughout its lifecycle.

EU NIS2 Directive (2022/2555)

- **Article 21(2)(a)**: Obligates 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.

EU DORA (2022/2554)

- **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's governance expectations.

COBIT 2019

- **EDM01 – Governance Framework Setting**: This policy supports enterprise governance by defining ISMS roles, leadership commitments, and strategic objectives.
- **APO01 – Management Framework**: Supports the establishment and operation of a structured ISMS.
- **APO12 – Risk Management**: Provides the foundation for information security risk governance.
- **MEA01/MEA03 – Monitor, Evaluate and Assess**: Reinforces continuous performance evaluation and internal control monitoring through policy compliance enforcement.