					[Insert Registered Legal Entity Name Here]							
Document number: P6S					Document Title: **Risk Management 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**

Aligned with standards and regulations where applicable		
Standard/Regulation	**Clause/Article**	**Comment**
ISO/IEC 27001:2022	Clauses 6.1, 6.1.3	
ISO/IEC 27002:2022	5.4, 5.25	
NIST SP 800-53 Rev.5	RA-1 to RA-7, PM-9	
EU NIS2	Article 21(2)(a–d)	
EU DORA	Article 5	
COBIT 2019	APO12, MEA0	

					[Insert Registered Legal Entity Name Here]							
Document number: P6S					Document Title: **Risk Management Policy**							
Version: 1.0		Effective Date: 01.01.2025			Document Owner:							
X	Policy		Standard		Procedure		Form		Register		Other	

Purpose

1.1. This policy defines how the organization identifies, evaluates, and manages risks related to information security, operations, technology, and third-party services.

1.2. It ensures that risk management is an active part of planning, project execution, vendor selection, and incident response, in alignment with ISO 27001, ISO 31000, and regulatory requirements.

1.3. The policy supports informed decision-making, protection of information assets, and resilience of key business operations.

2. Scope

2.1. This policy applies to:

2.1.1. All departments, systems, and users within the organization

2.1.2. All information, services, and assets managed internally or via third parties

2.1.3. Risk-related activities including project reviews, system upgrades, outsourcing, and regulatory compliance

2.2. It includes all types of risks, such as:

2.2.1. Cybersecurity threats and system vulnerabilities

2.2.2. Operational disruptions and service outages

2.2.3. Legal, compliance, or reputational exposures

2.2.4. Third-party and supply chain risks

2.3. All employees, contractors, and service providers must follow this policy when identifying or reporting risks.

3. Objectives

3.1. Integrate simple and repeatable risk assessment procedures into normal business operations.

3.2. Identify and prioritize risks that could impact confidentiality, integrity, availability, or legal compliance.

3.3. Assign ownership and define treatment actions for all significant risks.

3.4. Maintain an accurate and up-to-date Risk Register to support audit readiness and risk tracking.

3.5. Ensure management involvement in approving risk tolerance and major treatment plans.

4. Roles and Responsibilities

4.1. **General Manager**

4.1.1. Sets the organization's risk appetite and endorses the risk management framework.

4.1.2. Approves major risk treatment decisions and resources.

4.1.3. Reviews the top risks quarterly with the Risk Coordinator.

4.2. **Risk Coordinator (or ISMS Owner)**

4.2.1. Facilitates risk assessments and maintains the Risk Register.

4.2.2. Ensures that risk scoring, ownership, and treatment actions are documented.

4.2.3. Organizes at least one formal risk review per year.

4.3. **Department Heads / Business Process Owners**

4.3.1. Identify risks in their operational area and propose mitigation plans.

4.3.2. Own the resolution and ongoing monitoring of those risks.

4.4. **IT Support / Service Providers**

4.4.1. Analyze technical and cyber risks, assist with risk mitigation implementation.

4.4.2. Participate in assessments of software, hardware, and infrastructure changes.

4.5. **Employees and Contractors**

4.5.1. Report suspected risks or security incidents to the Risk Coordinator.

4.5.2. Follow assigned controls or mitigation actions for known risks.

5. Governance Requirements

5.1. **Risk Register Maintenance**

5.1.1. All identified risks must be logged in the Risk Register.

5.1.2. Each risk must include: description, likelihood, impact, score, owner, and treatment plan.

5.1.3. Risks must be reviewed quarterly and updated when significant events occur.

5.2. **Risk Assessment Timing**

[…….]