					[Insert Registered Legal Entity Name Here]							
Document number: P2S					Document Title: **Governance Roles & Responsibilities 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	Clause 5.3	
ISO/IEC 27002:2022	Controls: 5.2, 5.3, 5.4	
NIST SP 800-53 Rev.5	PM-1, PL-1, PL-4, CA-1, AC-1	
EU GDPR	Articles 5(2), 32	

					[Insert Registered Legal Entity Name Here]								
Document number: P2S					Document Title: **Governance Roles & Responsibilities Policy**								
Version: 1.0		Effective Date: 01.01.2025			Document Owner:								
X	Policy		Standard		Procedure		Form		Register		Other		

1. **Purpose**
   1.1. This policy defines how governance responsibilities for information security are assigned, delegated, and managed in the organization to ensure full compliance with ISO/IEC 27001:2022 and other regulatory obligations.
   1.2. It ensures accountability at every level and supports operational effectiveness by clearly identifying who is responsible for each security-related function.
   1.3. This policy enhances audit readiness and builds customer trust by demonstrating formal security governance, even in organizations with limited technical staff or outsourced IT.
2. **Scope**
   2.1. This policy applies to all individuals who handle organizational systems or data, including:
      2.1.1. Business owners, general managers
      2.1.2. Employees and contractors
      2.1.3. External IT service providers or consultants
   2.2. It covers all systems, environments, and services used to process, transmit, or store business or customer information, including:
      2.2.1. Office IT infrastructure and remote work devices
      2.2.2. Cloud-based platforms and email services
      2.2.3. Physical records and shared drives
   2.3. The scope includes both internal and outsourced activities involving information security governance.
3. **Objectives**
   3.1. Establish clear accountability for all security-related duties, including policy management, access control, incident handling, and monitoring.
   3.2. Enable effective separation of duties to reduce conflicts of interest or fraud risks.
   3.3. Ensure security tasks and roles are clearly documented and reviewed regularly.
   3.4. Enable informed decision-making, escalation, and oversight of IT and security risks.
   3.5. Support ISO/IEC 27001:2022 certification and build confidence among customers, partners, and auditors.
4. **Roles and Responsibilities**
   4.1. **General Manager / Business Owner**
      4.1.1. Has full responsibility for the implementation and oversight of this policy.
      4.1.2. Approves all security roles, responsibilities, and delegation decisions.
      4.1.3. Monitors compliance and makes final decisions on policy exceptions and escalations.
   4.2. **Designated Security Coordinator (if assigned)**
      4.2.1. May be a staff member or trusted consultant.
      4.2.2.This role may be assumed by the General Manager or an external provider in micro-business environments
      4.2.3. Assists with day-to-day enforcement of access control, incident response, or basic technical security tasks.
      4.2.4. Reports directly to the General Manager on any security issues or risks.
   4.3. **External IT Service Provider**

4.3.1. Implements security controls, maintains infrastructure, and monitors for unauthorized access.
4.3.2. Is contractually bound to follow all security requirements of the organization.

[……..]