					Insert Registered Legal Entity Name Here							
Document number: P02S					Document Title: **Governance Roles and 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

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clause 5	
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	

1. Purpose

1.1 This policy defines how information security governance responsibilities are assigned, delegated, and managed within the organization to ensure compliance with ISO/IEC 27001:2022 and other regulatory obligations.

1.2 It establishes accountability at every level and supports operational effectiveness by clearly defining responsibility for each security-related function.

1.3 This policy enhances audit readiness and supports customer confidence by demonstrating formal security governance, including in organizations with limited technical personnel or outsourced IT services.

2. Scope

2.1 This policy applies to all individuals who handle organizational systems or data, including:

2.1.1 Business owners and general managers

2.1.2 Employees and contractors

2.1.3 External IT service providers or consultants

2.2 It applies to all systems, environments, and services used to process, transmit, or store business or customer information, including:

2.2.1 Office IT infrastructure and remote working 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 related to 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 segregation of duties to reduce the risk of conflicts of interest or fraud.

3.3 Ensure security tasks and roles are clearly documented and reviewed regularly.

3.4 Support 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 overall 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 an employee or a trusted consultant.

4.2.2 This role may be performed by the General Manager or an external provider in micro-business environments.

4.2.3 Supports day-to-day enforcement and compliance activities related to access control, incident response, or basic technical security tasks.

4.2.4 Reports directly to the General Manager on security issues or risks.

[... 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 Annual Review

9.1.1 This policy must be reviewed by the General Manager every 12 months to ensure that it continues to reflect legal obligations, operational needs, and ISO/IEC 27001 certification requirements.

9.2 Interim Reviews

9.2.1 Reviews must also be performed when:

9.2.1.1 There are major organizational changes

9.2.1.2 A new provider is onboarded

9.2.1.3 A serious security incident occurs

9.2.1.4 Regulations such as GDPR, NIS2, or DORA are updated

9.3 Version Control and Documentation

9.3.1 All reviews must include:

9.3.1.1 Date of review

9.3.1.2 Summary of any changes

9.3.1.3 Signature or documented approval by the General Manager

9.3.1.4 Archived prior versions for audit reference

9.4 Communication of Changes

9.4.1 All policy updates must be communicated promptly to staff and providers by email, internal portals, or formal memoranda.

10. Related Policies and Linkages

10.1 This policy should be implemented alongside the following SME policies to ensure full effectiveness:

10.1.1 P4S – Access Control Policy: Defines how access is granted, managed, and revoked, and is directly linked to assigned roles and oversight.

10.1.2 P8S – Information Security Awareness and Training Policy: Reinforces role-specific responsibilities and expectations.

10.1.3 P17S – Data Protection and Privacy Policy: Defines legal duties under GDPR assigned to roles established in this governance policy.

10.1.4 P30S – Incident Response Policy: Requires defined responsibilities for incident reporting, escalation, and resolution.

10.2 Together, these policies support consistent enforcement and compliance, internal accountability, and external compliance.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001

11.1.1 Clause 5.3 – Organizational Roles, Responsibilities and Authorities: Requires roles to be clearly assigned and supported by top management.

11.2 ISO/IEC 27002

11.2.1 Controls 5.2–5.4: Require clear documentation of information security roles, segregation of duties, and management oversight.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1: Establishes an overarching information security program with defined responsibilities.

11.3.2 PL-1 to PL-4: Require planning controls, including policy development and documented role assignments.

11.3.3 CA-1: Requires defined assessment and authorization roles.

11.3.4 AC-1: Links role-based access control to assigned governance responsibilities.

11.4 EU GDPR

11.4.1 Article 5(2) – Accountability: Requires organizations to demonstrate compliance through defined roles and responsibilities.

11.4.2 Article 32 – Security of Processing: Emphasizes clear assignment of duties to protect personal data.

11.5 EU NIS

11.5.1 Article 21(2)(a): Requires governance structures that include formalized roles for managing cyber risk and incidents.

11.6 EU DORA

11.6.1 Articles 9 and 10: Require financial entities to clearly assign and oversee ICT- and security-related responsibilities.

11.7 COBIT 2019

11.7.1 EDM03 – Ensure Risk Optimization: Requires well-defined roles and escalation routes for managing security risk.

11.7.2 APO13 – Manage Security: Assigns strategic and operational security duties to individuals and roles.

11.7.3 DSS05 – Manage Security Services: Requires structure and traceability in responsibilities for external and internal security services.