					Insert Registered Legal Entity Name Here							
Document number: P01S					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**

Aligned with standards and regulations

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clauses 5.1, 5.2, 5.3, 6.1, 6.2, 8	Specifies management commitment, policy requirements, role assignment, risk assessment, and operational control
ISO/IEC 27002:2022	Controls 5.1–5.5	Specifies the establishment of documented information security policies, assignment of roles, segregation of duties, and management responsibilities
NIST SP 800-53 Rev.5	PM-1, PL-1, CA-1, AC-1	Requirements for the security program plan, security planning policy, assessment and authorization, and access control
EU GDPR (2016/679)	Article 5(2), Article 32	Accountability principle and security of processing measures, particularly for documented roles
EU NIS2 Directive (2022/2555)	Article 21(2)(a)	Requires risk management measures, roles, and responsibilities for cyber risk management
EU DORA (2022/2554)	Article 9, Article 10	Requires assignment of roles for ICT risk management and business continuity
COBIT 2019	EDM03, APO13, DSS05	Ensures risk optimization, security management, and security services management through clear role assignment

1. Purpose

1.1 This policy demonstrates the organization’s commitment to protecting customer and business information by clearly defining responsibilities and practical security measures appropriate for organizations without dedicated IT teams.

1.2 It ensures that all employees, contractors, and service providers comply with enforceable requirements, enabling full compliance with ISO/IEC 27001 certification requirements.

1.3 This policy enables the organization to build customer trust by clearly demonstrating how information is protected through defined responsibilities, structured processes, and clear accountability.

2. Scope

2.1 This policy applies to all individuals who access or manage the organization’s data and systems, including:

2.1.1 Business owners and general managers

2.1.2 Employees, contractors, and interns

2.1.3 External IT service providers or consultants

2.2 It applies to all types of information, systems, and services, including:

2.2.1 Business records, customer data, passwords, and emails

2.2.2 IT assets such as laptops and mobile phones

2.2.3 Cloud services used for file storage, communication, or finance

2.2.4 Physical documents stored at office locations

2.3 This policy applies across all working environments—office-based, remote, and cloud-based—and includes all devices and software used to process or store business information.

3. Objectives

3.1 Assign Clear Responsibility: Ensure that accountability for information security is always assigned. Typically, this is the General Manager or a person formally designated by the General Manager.

3.2 Protect Customer and Business Information: Implement reliable and consistent safeguards to prevent misuse, loss, or theft of sensitive information, including customer and financial records.

3.3 Support ISO/IEC 27001 Certification: Enable the organization to demonstrate full compliance with ISO/IEC 27001 requirements, ensuring audit readiness and certification eligibility without requiring complex infrastructure.

3.4 Embed Security in Business Operations: Integrate information security into day-to-day activities and decision-making across the organization.

3.5 Build Security Awareness and Culture: Ensure that every employee understands and follows security practices, such as using strong passwords and reporting suspicious activity.

4. Roles and Responsibilities

4.1 General Manager or Business Owner

4.1.1 Retains overall accountability for information security.

4.1.2 Approves, maintains, and reviews this policy.

4.1.3 Ensures that all key security tasks are either performed directly or formally delegated in writing.

4.1.4 Verifies that any delegated security tasks, such as access management or incident response, are carried out effectively.

4.1.5 Acts as the default contact for all internal and external security matters, including audits and customer inquiries.

4.1.6 Monitors progress against these objectives during the annual review. Objectives must be measurable where practicable (e.g., percentage of staff trained, number of incidents reported) and revised based on security findings and changes in risk.

4.2 Designated Employee (if applicable)

4.2.1 May support the General Manager in carrying out day-to-day tasks, such as creating user accounts, removing access for leavers, or coordinating with the IT service provider.

4.2.2 Must be formally assigned and provided with sufficient authority and tools to perform the assigned tasks.

4.2.3 Must report any issues to the General Manager.

[... 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 (GM) at least annually to ensure continued compliance with ISO/IEC 27001 certification requirements, regulatory changes (such as GDPR, NIS2, and DORA), and evolving business needs.

9.2 Interim Reviews

9.2.1 Additional reviews must be conducted whenever significant changes occur, such as:

9.2.1.1 Major security incidents or breaches

9.2.1.2 Introduction of new business processes or technologies (e.g., new software, remote working platforms, or cloud services)

9.2.1.3 Changes in legal or regulatory requirements affecting information handling

9.3 Documentation of Changes

9.3.1 All policy reviews and changes must be formally documented, clearly stating the date, nature of the revisions, and the GM's approval.

9.3.2 A historical record of policy versions must be securely maintained to demonstrate policy evolution and compliance during audits.

9.4 Communication of Updates

9.4.1 Any changes to this policy must be communicated promptly to all employees, contractors, and relevant third parties.

9.4.2 Updated versions of the policy must be readily accessible to all affected personnel (e.g., shared electronically or physically posted in the workplace).

10. Related Policies and Linkages

10.1 This policy is closely linked to other policies in the organization's SME policy set, specifically:

10.1.1 P2S – Governance Roles & Responsibilities Policy: Clarifies the assignment of security duties and responsibilities.

10.1.2 P4S – Access Control Policy: Defines secure management of access to company information.

10.1.3 P8S – Information Security Awareness and Training Policy: Provides essential guidance for staff training and awareness.

10.1.4 P17S – Data Protection and Privacy Policy: Ensures compliance with GDPR and other data protection legislation.

10.1.5 P30S – Incident Response Policy: Describes the detailed actions required in response to security incidents.

10.2 These related policies provide clear operational guidance and must be implemented collectively to achieve full compliance with ISO/IEC 27001 certification requirements.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001

11.1.1 Clause 5.1 – Leadership and Commitment: Requires top management commitment and accountability for the effectiveness of information security within the organization.

11.1.2 Clause 5.2 – Information Security Policy: Requires clear, documented policies aligned with organizational strategy and compliance requirements.

11.1.3 Clause 5.3 – Organizational Roles and Responsibilities: Defines the clear assignment of information security responsibilities across the organization, which is essential for effective governance and audit compliance.

11.1.4 Clause 6.1 – Actions to Address Risks and Opportunities: Ensures that information security risks and opportunities are systematically identified, evaluated, and treated.

11.1.5 Clause 8.1 – Operational Planning and Control: Requires the organization to plan and implement the processes needed to meet information security objectives and manage associated risks effectively.

11.2 ISO/IEC 27002:2022 Controls 5.1–5.5

11.2.1 Annex A Control 5.1 – Policies for Information Security: Specifies the development and communication of documented information security policies.

11.2.2 Annex A Control 5.2 – Information Security Roles: Clarifies and formally assigns information security roles and responsibilities to relevant parties.

11.2.3 Annex A Control 5.3 – Segregation of Duties: Requires clear segregation of duties to reduce conflicts of interest and fraud risk in the management of sensitive information.

11.2.4 Annex A Control 5.4 – Management Responsibilities: Requires management to demonstrate commitment to information security through active oversight and resource allocation.

11.2.5 Annex A Control 5.5 – Contact with Authorities: Reinforces the need for clearly documented information security responsibilities and governance arrangements that support consistent management and audit traceability across the organization.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1 – Information Security Program Plan: Requires documented information security governance strategies and policies, providing a framework for consistent implementation and management.

11.3.2 PL-1 – Security Planning Policy: Requires an organization-wide security planning policy to support secure operations and strategic alignment of information security activities.

11.3.3 CA-1 – Security Assessment and Authorization Policy: Requires clearly defined assessment and authorization roles to ensure ongoing effectiveness and compliance with information security requirements.

11.3.4 AC-1 – Access Control Policy: Requires organizations to clearly define, document, and enforce access management practices and responsibilities.

11.4 EU GDPR (2016/679)

11.4.1 Article 5(2) – Accountability Principle: Requires organizations to demonstrate compliance with data protection principles, including documented roles and policies for data protection responsibilities.

11.4.2 Article 32 – Security of Processing: Requires the implementation of appropriate technical and organizational measures, including clear security responsibilities, to protect personal data against breaches and unauthorized access.

11.5 EU NIS2 Directive (2022/2555)

11.5.1 Article 21(2)(a) – Risk Management Measures: Requires clear governance arrangements, including defined roles and responsibilities for information security, that are essential to effective cyber risk management.

11.6 EU DORA (2022/2554)

11.6.1 Article 9 – ICT Risk Management: Requires organizations to clearly assign roles and responsibilities relating to ICT risk management, thereby strengthening resilience and business continuity preparedness.

11.6.2 Article 10 – ICT Business Continuity: Requires clear accountability and structured roles for maintaining ICT resilience and continuity, ensuring that organizations can respond reliably to disruptions.

11.7 COBIT 2019

11.7.1 EDM03 – Ensure Risk Optimization: Emphasizes clearly defined accountability and roles in managing organizational risks, providing strong governance and effective oversight of information security risks.

11.7.2 APO13 – Manage Security: Requires organizations to clearly establish and communicate security management responsibilities, ensuring alignment with business objectives and regulatory requirements.

11.7.3 DSS05 – Manage Security Services: Requires structured roles and clear responsibilities for managing security services, enabling consistent implementation and compliance verification.