					[Insert Registered Legal Entity Name Here]								
Document number: P13					Document Title: **Data Classification and Labeling 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 4.2, 6.1.3, 7.2, 7.3, 7.5, 8.1	
ISO/IEC 27002:2022	Controls 5.9–5.14, 8.11–8.12	
NIST SP 800-53 Rev.5	AC-16, MP-3, MP-5, PL-2	
EU GDPR	Articles 5, 32	
EU NIS2	Articles 21(2)(a), 21(3)	
EU DORA	Articles 5, 9	
COBIT 2019	DSS05.02, MEA03	

					[Insert Registered Legal Entity Name Here]									
Document number: P13					Document Title: **Data Classification and Labeling 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 the formal framework for classifying and labeling organizational information assets based on sensitivity, risk exposure, and regulatory obligations.

1.2 It ensures that all information—whether stored, transmitted, or processed—is clearly categorized and labeled in a manner that communicates its required level of protection and handling.

1.3 The policy enforces structured classification aligned with the organization's risk management practices, supporting confidentiality, integrity, and availability goals across both digital and physical data types.

1.4 This control is essential for enabling role-based access, audit readiness, appropriate data sharing, and the effective deployment of technical safeguards such as encryption, backup, and monitoring.

2. Scope

2.1 This policy applies to:

2.1.1 All organizational information assets, including documents, databases, records, and communications

2.1.2 All data formats, including digital, printed, written, or verbal

2.1.3 All environments: on-premises, remote, mobile, and cloud

2.1.4 All employees, contractors, service providers, and third-party processors who create, handle, or store organizational information

2.2 The scope encompasses internally developed content, externally sourced data, personal data under privacy law obligations (e.g., GDPR), and information exchanged with clients, partners, and regulators.

2.3 It applies to all systems used to store or transmit data, including enterprise applications, file servers, email systems, cloud platforms, and backup repositories.

3. Objectives

3.1 To establish a standardized, organization-wide classification scheme based on the impact of data exposure or compromise.

3.2 To ensure all information is visibly and persistently labeled to reflect its classification level and handling requirements.

3.3 To enforce data handling and access controls aligned with classification, including encryption, logging, transmission protection, and retention scheduling.

3.4 To support compliance with international standards (ISO/IEC 27001, 27002), legal frameworks (GDPR, NIS2, DORA), and internal risk policies.

3.5 To ensure that all users understand their responsibilities in protecting data, applying labels, and handling classified information correctly.

3.6 To maintain traceability between classification status, associated controls, and the organization's asset inventory for audit and compliance purposes.

4. Roles and Responsibilities

4.1 Chief Information Security Officer (CISO)

4.1.1 Owns the information classification and labeling policy and ensures it aligns with regulatory, contractual, and operational requirements.

4.1.2 Approves classification levels, labeling standards, and policy revisions.

4.1.3 Oversees policy compliance through audits, metrics, and exception reviews.

[….]

11. Reference Standards and Frameworks

This policy is aligned with internationally recognized standards and regulatory frameworks governing the classification and labeling of sensitive information.

ISO/IEC 27001:2022

Clause 4.2 – Understanding the Needs and Expectations of Interested Parties. Classification requirements often stem from legal, regulatory, or contractual obligations imposed by interested parties (e.g., GDPR, client NDAs), which must be reflected in the policy.

Clause 6.1.3 – Information Security Risk Treatment. Classification directly impacts the selection of risk treatment controls, including access control, encryption, and retention, based on data sensitivity.

Clause 7.2 – Competence. The policy mandates that personnel responsible for classification and labeling must be trained, which falls under competence requirements.

Clause 7.3 – Awareness. The policy requires all users to be aware of classification tiers and their responsibilities in handling information, aligning with awareness obligations.

Clause 7.5 – Documented Information. The classification policy itself is a controlled document, and the procedures, training records, and classification labels are part of documented information.

Clause 8.1 – Operational Planning and Control. Classification and labeling are operational processes embedded into data lifecycle management, and this clause ensures that such activities are planned, implemented, and controlled.

Clause 9.1 – Monitoring, Measurement, Analysis and Evaluation. The policy includes provisions for monitoring classification compliance, incident trends, and the effectiveness of the labeling scheme.

Clause 10.1 – Nonconformity and Corrective Action. The policy defines responses to misclassification, including corrective actions like retraining, updates, and exception handling.

ISO/IEC 27002:2022 – Controls 5.12 and 5.13

5.12 – Classification of Information. This control ensures that information is classified based on its sensitivity, value, and criticality—precisely what this policy formalizes.

5.13 – Labelling of Information. This control requires appropriate labeling of information in accordance with its classification level, fully addressed in the policy.

5.10 – Acceptable Use of Information and Other Associated Assets. The policy enforces how users should handle classified data, directly supporting acceptable use and preventing misuse.

5.11 – Return of Assets. Classification helps ensure sensitive data is identified and securely returned or sanitized when an employee or vendor departs.

5.9 – Inventory of Information and Other Associated Assets. Classification is often tied to the asset inventory, which must reflect the classification level of each item to support proper control allocation.

5.14 – Information Transfer. Classification levels influence controls on internal and external data transfers (e.g., encryption, approval, access restrictions).

8.12 – Data Leakage Prevention. Enforcing classification and labeling supports the prevention of unauthorized disclosure and data loss.

8.11 – Data Masking. Certain classification levels (e.g., Confidential, Restricted) may mandate masking when data is used in test/dev or analytics.

NIST SP 800-53 Rev.5

PL-2 – System and Communications Protection Policy and Procedures: Supports classification policies as part of overarching data protection.

AC-16 – Security Attributes: Implements access enforcement based on classification metadata and user permissions.

MP-3 / MP-5 – Media Marking and Transport Protection: Enforces labeling and protection of data at rest and in transit based on classification.

EU GDPR (2016/679)

Article 5 – Data Protection Principles: Requires personal data to be processed securely, proportionate to its sensitivity.

Article 32 – Security of Processing: Reinforces classification as a mechanism for risk-based data protection and appropriate technical measures.

EU NIS2 Directive (2022/2555)

Article 21(2)(a): Requires policies for information security risk management, including asset and data classification controls.

Article 21(3): Encourages adoption of measures to enforce appropriate data handling—supported through classification-based labeling.

EU DORA (2022/2554)

Article 5 – Governance and Control: Requires governance frameworks that classify data assets for ICT risk control.

Article 9 – ICT Risk Management: Imposes technical and organizational measures for critical ICT assets, including classification and labeling.

COBIT 2019

DSS05.02 – Manage Security Services: Enforces information security classifications to ensure protection of enterprise data.

MEA03 – Monitor, Evaluate, and Assess Compliance: Supports regular audit and review of classification practices to ensure policy adherence and maturity.