<table>
<tr><td colspan="4"></td><td colspan="8">[Insert Registered Legal Entity Name Here]</td></tr>
<tr><td colspan="4">Document number:
P13S</td><td colspan="8">Document Title:
<b>Data Classification and Labeling Policy</b></td></tr>
<tr><td colspan="2">Version:
1.0</td><td colspan="2">Effective Date:
01.01.2025</td><td colspan="8">Document Owner:</td></tr>
<tr><td>X</td><td>Policy</td><td></td><td>Standard</td><td></td><td>Procedure</td><td></td><td>Form</td><td></td><td>Register</td><td></td><td>Other</td></tr>
</table>

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 5.3, 8.1	
ISO/IEC 27002:2022	Controls 5.12, 5.13	
NIST SP 800-53 Rev.5	AC-16, MP-3, MP-5	
EU NIS2	Article 21(2)(a)	
EU DORA	Article 5(8)	
COBIT 2019	BAI03.05, DSS05.02	
EU GDPR	Article 5, 32	

					[Insert Registered Legal Entity Name Here]						
Document number: P13S					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 how all information handled by the organization must be classified and labeled to ensure its confidentiality, integrity, and availability are maintained throughout its lifecycle.

1.2. It enables consistent data handling by assigning appropriate protection levels to information based on sensitivity, business impact, or legal obligations.

1.3. Classification and labeling help reduce the risk of accidental disclosure, unauthorized access, or mishandling of sensitive data, especially within SMEs that may rely on simpler systems and fewer formalized controls.

1.4. This policy is critical for ISO/IEC 27001 certification and regulatory compliance, particularly with data protection laws such as GDPR and cybersecurity frameworks like NIS2 and DORA.

2. Scope

2.1. This policy applies to all organizational data, regardless of format or location, including:

2.1.1. Electronic documents, spreadsheets, emails, forms, images, and scanned files

2.1.2. Physical documents such as printed records, reports, invoices, and notes

2.1.3. Data stored or processed in cloud services, on local servers, removable media, or personal devices used for business

2.1.4. Temporary or transitory data generated during business operations (e.g., logs, cache files, emails)

2.2. All staff, contractors, temporary workers, and external providers with access to organizational data are required to comply with this policy.

2.3. It applies throughout the data lifecycle—from creation and storage, through access and transfer, to archival or deletion.

3. Objectives

3.1. Define a simple, enforceable classification scheme that can be easily understood and applied across the organization.

3.2. Require every data asset to be classified according to its sensitivity and labeled accordingly to guide proper handling, storage, and access.

3.3. Ensure data labeling practices are integrated into business workflows such as onboarding, project launch, and system setup.

3.4. Reduce the risk of data breaches by applying handling controls (e.g., encryption, access restriction) according to the classification level.

3.5. Ensure compliance with privacy and information security laws by demonstrating that sensitive data (e.g., personal, financial, or proprietary) is properly labeled and managed.

3.6. Establish accountability for classification decisions and ensure periodic reviews and updates based on evolving business and legal needs.

4. Roles and Responsibilities

4.1. **General Manager (GM)**

4.1.1. Owns this policy and approves the classification scheme.

4.1.2. Provides oversight to ensure classification responsibilities are delegated and enforced.

4.1.3. Must review and authorize any exceptions to classification or labeling requirements.

4.1.4. Ensures that data handling practices meet compliance requirements under laws such as GDPR and DORA.

4.2. **Information Owner / Data Manager**

4.2.1. Assigns an initial classification to each new data set or information asset upon creation or acquisition.

4.2.2. Ensures visible labels (e.g., file headers, footers, watermarks, folder names) are applied where applicable.

4.2.3. Reviews classifications periodically to verify relevance, accuracy, and any required changes (e.g., after declassification or publishing).

4.2.4. Works with the IT Lead to enforce technical protections based on classification (e.g., access rights, encryption).

4.3. **IT Lead or Administrator (internal or outsourced)**

4.3.1. Implements technical labeling features in file systems, cloud tools, or communication platforms.

4.3.2. Applies or enforces restrictions based on data classification (e.g., encryption, MFA, restricted folders).

4.3.3. Supports visibility of classification labels in metadata, shared drives, or backup systems.

4.3.4. Assists in training and verifying that classification tools or templates are being used correctly.

4.4. **All Employees and Contractors**

4.4.1. Must understand and apply the organization’s classification scheme.

4.4.2. Are responsible for checking and respecting classification labels before sharing, printing, storing, or transferring data.

4.4.3. Must report any unlabeled sensitive information or misclassified assets to the GM or Data Manager.

4.4.4. Are required to participate in training and policy acknowledgment activities.

5. . Governance Requirements

5.1. The organization must use a minimum three-tier classification model, as follows:

5.1.1. **Public**: Information approved for open sharing (e.g., website content, published brochures).

5.1.2. **Internal**: Business information restricted to staff and authorized contractors (e.g., internal procedures, project data).

5.1.3. **Confidential**: Sensitive data including personal information (PII), financial records, HR files, client data, or intellectual property.

5.2. All data classified as “Confidential” must receive the highest level of protection:

5.2.1. Access must be limited to named users with a need to know

5.2.2. Files must be stored in secured locations (e.g., access-controlled folders, encrypted drives)

5.2.3. External sharing must be explicitly authorized and logged

5.3. Labels must be applied visibly on all Confidential and Internal documents where feasible:

5.3.1. For electronic files: use headers, footers, file names, metadata tags

5.3.2. For physical documents: apply stamps, printed headers, or stickers

5.3.3. For systems: folders and databases should be named and segmented according to classification level

5.4. Classification must be reviewed during major events, such as:

5.4.1. Changes to business model, customer base, or product line
5.4.2. Onboarding of a new system, supplier, or contractor
5.4.3. Legal or regulatory changes that affect data handling requirements

6. **Policy Implementation Requirements**
   6.1. **Classification at Point of Creation**
   6.2. [……]

Reference Standards and Frameworks

ISO/IEC 27001:2022

Clause 5.3: Requires clearly defined responsibilities for data handling and protection.

Clause 8.1: Enforces operational planning and controls, including those tied to data categorization.

ISO/IEC 27002:2022

Control 5.12: Provides guidance on information classification based on risk and regulatory requirements.

Control 5.13: Details practical labeling mechanisms and associated handling rules.

NIST SP 800-53 Rev.5

AC-16: Requires marking of information to ensure that protection measures align with classification.

MP-3 / MP-5: Provide guidance on labeling and controlling media and outputs.

EU GDPR

Articles 5 and 32: Enforce data minimization and integrity through appropriate classification and handling safeguards.

EU NIS2

Article 21(2)(a): Mandates technical and organizational controls for risk-based data protection.

EU DORA

Article 5(8): Requires firms to classify data assets as part of their ICT risk management program.

COBIT 2019

BAI03.05: Calls for information classification and risk-adjusted protection.

DSS05.02: Addresses enforcement of classification-based controls and monitoring.

					[Insert Registered Legal Entity Name Here]						
Document number: P13S					Document Title: **Data Classification and Labeling Policy**						
Version: 1.0		Effective Date: 01.01.2025			Document Owner:						
X	Policy		Standard		Procedure		Form		Register		Other