| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Insert Registered Legal Entity Name Here | | | | | | | |
| Document number:<br>P13S | | | | | Document Title:<br>**Data Classification and Labeling Policy** | | | | | | | |
| Version:<br>1.0 | | Effective Date:<br>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 5.3, 8 | |
| ISO/IEC 27002:2022 | Controls 5.12, 5 | |
| 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 | |
| EU GDPR | Article 5, 32 | |

**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 establishes 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, particularly within SMEs that may rely on simpler systems and fewer formalized controls.

1.4 This policy is critical to ISO/IEC 27001 certification and regulatory compliance, particularly with data protection laws such as the GDPR and cybersecurity frameworks such as 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 purposes

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

2.2 All staff, contractors, third-party service providers, temporary workers, and external providers with access to organizational data must comply with this policy.

2.3 This policy applies throughout the data lifecycle, from creation and storage through access and transfer to archiving or deletion.

**3. Objectives**

3.1 Define a simple, enforceable classification scheme that can be readily 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 processes such as onboarding, project initiation, and system implementation.

3.4 Reduce the risk of data breaches by applying handling controls (e.g., encryption, access restrictions) in accordance with the classification level.

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

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

**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 assigned 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 applicable compliance obligations under laws such as the GDPR and DORA.

**4.2 Information Owner / Data Manager**

4.2.1 Assigns an initial classification to each new dataset 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 confirm continued relevance, accuracy, and any required changes (e.g., following declassification or publication).

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

[ ... 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 This policy must be reviewed annually by the GM and Data Manager to ensure it reflects:**

9.1.1 Changes in business operations or data types

9.1.2 New regulatory requirements (e.g., data privacy or financial oversight)

9.1.3 Technology changes affecting labeling or classification capabilities

9.2 The review must include updates to classification categories, labeling tools or practices, and awareness and training content.

9.3 Policy revisions must be approved by the GM and communicated to all staff. A record of version changes must be retained for audit purposes.

**10. Related Policies and Linkages**

10.1 P2S – Governance Roles and Responsibilities Policy: Assigns accountability for policy ownership and enforcement.

10.2 P4S – Access Control Policy: Aligns system access with data classification levels.

10.3 P12S – Asset Management Policy: Tracks the physical and digital assets that store classified data.

10.4 P17S – Data Protection and Privacy Policy: Governs the protection of personal data, much of which is classified as Confidential.

10.5 P30S – Incident Response Policy: Defines escalation paths and response procedures in the event of classification violations or data exposure.

**11. Reference Standards and Frameworks**

**11.1 ISO/IEC 27001**

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

11.1.2 Clause 8.1: Requires operational planning and controls, including those related to data classification.

**11.2 ISO/IEC 27002**

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

11.2.2 Control 5.13: Specifies practical labeling mechanisms and associated handling requirements.

**11.3 NIST SP 800-53 Rev.5**

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

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

**11.4 EU GDPR**

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

**11.5 EU NIS**

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

**11.6 EU DORA**

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

**11.7 COBIT 2019**

11.7.1 BAI03.05: Requires information classification and risk-adjusted protection.

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