					Insert Registered Legal Entity Name Here							
Document number: P12					Document Title: **Asset Management 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**

1. Purpose

1.1 This policy establishes the mandatory organizational requirements for identifying, classifying, managing, and protecting information assets throughout their lifecycle. It supports enterprise-wide governance of hardware, software, data, cloud, and intangible information assets, including those in mobile, remote, and third-party-managed environments.

1.2 The purpose of this policy is to ensure complete visibility of the organization's information asset landscape, enabling effective security controls, assignment of ownership, alignment with compliance obligations, and proper decommissioning or disposal.

1.3 This policy aligns with ISO/IEC 27001:2022 Annex A.5.9 by requiring the maintenance of a centralized inventory of information and associated assets. It ensures accountability by assigning each asset to an owner and applying classification-based protection according to business sensitivity and regulatory requirements.

2. Scope

2.1 This policy applies to all employees, contractors, third-party vendors, and service providers who manage, use, access, store, or process information assets owned or controlled by the organization.

2.2 The scope includes all categories of assets, including:

2.2.1 Physical assets: laptops, desktops, mobile devices, removable media, printers, network equipment

2.2.2 Digital assets: software, applications, system images, databases, backup data, encryption keys

2.2.3 Information assets: structured and unstructured data, reports, emails, intellectual property

2.2.4 Cloud and virtual assets: IaaS, SaaS, PaaS environments, virtual machines, containers

2.2.5 Logical assets: domain names, licenses, user accounts, configuration baselines

2.3 This policy also applies to assets used in remote, hybrid, or outsourced environments, ensuring protection and visibility even where assets are not physically located on organizational premises.

3. Objectives

3.1 To maintain a complete, accurate, and current inventory of all organizational information assets, including defined ownership, classification, and location attributes.

3.2 To assign Asset Owners responsible for the classification, handling, and protection of the assets under their control, in accordance with data governance and information security policies.

3.3 To apply appropriate classification and labeling to all assets based on sensitivity, criticality, and regulatory considerations.

3.4 To protect assets in accordance with their classification and associated risk exposure, including requirements for storage, access, transmission, and disposal.

3.5 To enforce asset return and secure disposal procedures during employee offboarding, contract termination, or end of asset lifecycle.

3.6 To support compliance with frameworks such as ISO/IEC 27001, GDPR, NIS2, DORA, and COBIT 2019 through structured asset management and auditability.

4. Roles and Responsibilities

4.1 Top Management

4.1.1 Approves the Asset Management Policy and ensures that resources are allocated for its full implementation.

4.1.2 Retains ultimate accountability for ensuring that organizational assets are protected and managed in accordance with regulatory and contractual obligations.

4.2 Chief Information Security Officer (CISO)

4.2.1 Owns the Asset Management Policy and ensures its integration with the organization's broader Information Security Management System (ISMS).

4.2.2 Reviews exceptions and deviations from this policy and enforces risk-based mitigating measures.

4.2.3 Oversees periodic audits of asset classification, inventory integrity, and compliance with asset lifecycle requirements.

[... 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 shall be reviewed at least annually, or in response to:

9.1.1 Changes in legal or regulatory obligations affecting asset classification or inventory requirements

9.1.2 Introduction of new asset categories or management platforms (e.g., cloud-native CMDBs)

9.1.3 Internal audit findings or security incidents involving asset mismanagement

9.1.4 Organizational restructuring affecting ownership or lifecycle controls

9.2 The review process shall be initiated by the IT Asset Manager and coordinated with the CISO, Procurement, Legal and Compliance, and affected department heads.

9.3 Interim reviews may also be triggered by:

9.3.1 Acquisition or divestiture of business units

9.3.2 Vendor changes affecting third-party-managed assets

9.3.3 Technology refreshes involving bulk decommissioning or provisioning

9.4 All revisions to this policy must:

9.4.1 Be version controlled and stored in the ISMS repository

9.4.2 Be approved by Top Management

9.4.3 Include a summary of changes and the supporting rationale

9.4.4 Be communicated to all affected stakeholders, including updated procedures or system training, where applicable

10. Related Policies and Linkages

10.1 This policy operates in conjunction with, and supports enforcement of, the following related policies:

10.1.1 P4 - Access Control Policy: Ensures that asset visibility aligns with access entitlements and control mechanisms across systems and data environments.

10.1.2 P7 - Onboarding and Termination Policy: Governs timely provisioning and return of physical and logical assets during personnel transitions.

10.1.3 P13 - Data Classification and Labeling Policy: Establishes mandatory asset classification requirements that determine labeling, handling, and disposal procedures.

10.1.4 P14 - Data Retention and Disposal Policy: Defines the secure disposal timelines and methods for digital and physical information-bearing assets.

10.1.5 P22 - Logging and Monitoring Policy: Enables traceability of asset access and use through system logging, endpoint visibility, and behavioral analytics.

10.1.6 P30 - Incident Response Policy: Supports rapid containment and investigation of asset-related breaches, such as lost laptops or untracked storage media.

10.2 These policies form a cohesive governance framework to ensure that assets are securely managed, accurately inventoried, and appropriately handled throughout their lifecycle.

11. Reference Standards and Frameworks

11.1 This policy is aligned with internationally recognized information security standards and regulatory frameworks that require robust asset management throughout the lifecycle.

11.2 ISO/IEC 27001:

11.2.1 Clause 8.1 - Requires organizations to plan, implement, and control the processes necessary to meet information security requirements, including those relating to asset lifecycle management.

11.3 ISO/IEC 27002:2022 - Controls 5.9 to 5.

11.3.1 Clause 5.9 - Inventory of Information and Other Associated Assets: Requires a complete and up-to-date inventory of all assets relevant to information processing.

11.3.2 Clause 5.10 - Acceptable Use of Information and Assets: Supported through usage rules, ownership assignment, and return processes.

11.3.3 Clause 5.11 - Return of Assets: Implemented through formal handover and decommissioning procedures.

11.3.4 These controls establish structured requirements for identifying, labeling, maintaining, and tracking organizational assets, with corresponding responsibilities for owners and custodians throughout the lifecycle.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CM-8 - System Component Inventory: Reflected through centralized asset management, real-time visibility, and linkage to operational configurations.

11.4.2 RA-3 - Risk Assessment: Asset inventories serve as foundational inputs to threat modeling and risk assessment.

11.4.3 MP-6 - Media Sanitization: Enforced through secure disposal methods defined in asset lifecycle controls and the Data Disposal Policy.

11.5 EU GDPR (2016/679):

11.5.1 Article 30 - Records of Processing Activities: Requires organizations to document systems, devices, and repositories that store or process personal data.

11.5.2 Article 32 - Security of Processing: Aligns with asset-based risk evaluation and safeguards tailored to classified assets and critical infrastructure.

11.6 EU NIS2 Directive (2022/2555):

11.6.1 Article 21(2)(a, b): Mandates asset visibility and inventory as foundational elements of risk analysis, protection, and cybersecurity incident response.

11.6.2 Article 21(3): Reinforces the need for structured asset governance as part of the organization’s security culture.

11.7 EU DORA (2022/2554):

11.7.1 Article 5 - ICT Governance and Internal Control: Requires financial entities to control ICT assets through clear inventory, ownership, and protection requirements.

11.7.2 Article 9 - ICT Risk Management Framework: Establishes that asset management processes must support threat mitigation, continuity planning, and service resilience.

11.8 COBIT 2019:

11.8.1 BAI09 - Manage Assets: Directly aligned with the structured identification, classification, use, and disposal of enterprise assets.

11.8.2 DSS01 - Managed Operations: Supports implementation of controls that ensure asset protection and ongoing operational governance.

11.8.3 MEA03 - Monitor, Evaluate, and Assess Compliance: Ensures regular auditing of asset management controls and their effectiveness in achieving regulatory alignment.