					[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**

Aligned with standards and regulations where applicable		
Standard/Regulation	**Clause/Article**	**Comment**
ISO/IEC 27001:2022	Clause 8.1	
ISO/IEC 27002:2022	Controls 5.9 to 5.11	
NIST SP 800-53 Rev.5	CM-8, CM-6, MP-6	
EU GDPR	Articles 30, 32	
EU NIS2	Articles 21(2)(a, b), 21(3)	
EU DORA	Articles 5, 9	
COBIT 2019	BAI09, DSS01, MEA03	

					[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		

1. Purpose

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

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

1.3 The policy aligns with ISO/IEC 27001:2022 Annex A.5.9 by mandating the maintenance of a centralized inventory of information and associated assets. It ensures accountability by linking each asset to an owner and applying classification-driven protection based on 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, such as:

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 The policy also governs assets used in remote work, hybrid, or outsourced environments, ensuring protection and visibility even when assets are not physically located on organizational premises.

3. . Objectives

3.1 To maintain a complete, accurate, and up-to-date inventory of all organizational information assets, with 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 line with data governance and 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 according to their classification and associated risk exposure, including storage, access, transmission, and disposal.

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

3.6 To support regulatory 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 **Executive Management**

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

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

[……]

11. Reference Standards and Frameworks

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

ISO/IEC 27001:2022

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

ISO/IEC 27002:2022 - Controls 5.9 to 5.11

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

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

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

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

NIST SP 800-53 Rev.5

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

RA-3 - Risk Assessment: Asset inventories serve as foundational elements for threat modeling and risk evaluation.

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

EU GDPR (2016/679)

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

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

EU NIS2 Directive (2022/2555)

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

Article 21(3): Reinforces the necessity of structured asset governance as part of an organizational security culture.

EU DORA (2022/2554)

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

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

COBIT 2019

BAI09 - Manage Assets: Directly aligned to the structured identification, classification, usage, and disposal of enterprise assets.

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

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