					[Insert Registered Legal Entity Name Here]							
Document number: P12S					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	Control 5.9	
NIST SP 800-53 Rev.5	CM-8	
EU NIS2	Article 21(2)(a)	
EU DORA	Article 5(8)	
COBIT 2019	BAI09	
EU GDPR	Article 30	

1. **Purpose**
   1.1. This policy defines how the organization identifies, tracks, protects, and retires its information assets, including both physical and digital components.
   1.2. The aim is to reduce operational and security risks by maintaining visibility, accountability, and secure handling of all business assets throughout their lifecycle.
   1.3. A reliable asset inventory supports regulatory compliance, incident response, continuity planning, and risk management.
   1.4. This policy also supports certification under ISO/IEC 27001 and demonstrates alignment with legal, financial, and cybersecurity obligations under frameworks like GDPR, NIS2, and DORA.
   1.5. For small and medium-sized enterprises (SMEs), a simple but systematic asset management approach is essential to avoid unmanaged devices, data loss, or audit failure—especially when operating with limited technical staffing.
2. **Scope**
   2.1. This policy applies to all assets owned, leased, or otherwise managed by the organization, including those used in:
      2.1.1. Office-based work
      2.1.2. Remote or hybrid arrangements
      2.1.3. Field-based or mobile operations
      2.1.4. Cloud and outsourced environments
   2.2. Covered asset types include but are not limited to:
      2.2.1. **Hardware**: laptops, desktops, monitors, phones, tablets, USB drives, routers, printers, backup media
      2.2.2. **Software**: installed applications, SaaS tools, operating systems, antivirus tools, licenses
      2.2.3. **Data assets**: business data repositories, spreadsheets, customer records, source code
      2.2.4. **Digital credentials and services**: domain names, digital certificates, API keys, email accounts, cloud logins
      2.2.5. **Access devices**: keys, smartcards, access fobs, biometric tokens
   2.3. All employees, contractors, and third-party providers handling organizational assets fall within the scope of this policy.
   2.4. The policy also governs both short-term (e.g., project-specific laptops) and long-term assets, as well as shared assets used by multiple personnel.
3. **Objectives**
   3.1. Establish and maintain a complete, accurate inventory of all relevant assets, updated on a continuous basis.
   3.2. Ensure that each asset has a designated owner responsible for its use, storage, and return.
   3.3. Classify assets based on sensitivity, business impact, or regulatory relevance, enabling differentiated protection levels.
   3.4. Define clear procedures for asset issuance, reassignment, maintenance, loss reporting, and retirement.

3.5. Ensure assets are securely handled throughout their lifecycle and that information they store is either protected or securely erased upon disposal.
3.6. Reduce the likelihood of security incidents caused by untracked, unreturned, or misused organizational resources.
3.7. Support compliance with relevant laws (e.g., GDPR's accountability principle) and cybersecurity certification standards.

4. Roles and Responsibilities

4.1. **General Manager (GM)**
4.1.1. Owns this policy and is responsible for ensuring that asset management practices are implemented and followed across the organization.
4.1.2. Reviews and approves updates to the asset inventory and authorizes asset decommissioning or transfer where needed.
4.1.3. Must be notified of any significant loss, theft, or misuse of assets.

4.2. **IT Lead or Designated Asset Custodian**
4.2.1. Maintains the asset inventory (e.g., in a spreadsheet, ticketing system, or lightweight asset tracker).
4.2.2. Assigns asset ownership and tracks changes to status (e.g., new, in use, under repair, retired).
4.2.3. Verifies that all issued assets are documented and linked to an individual or business unit.
4.2.4. Ensures that classification labels are applied and followed (e.g., Internal, Confidential).
4.2.5. Coordinates retrieval, sanitization, and deactivation of assets during offboarding or retirement.
4.2.6. Reports any unresolved asset discrepancies to the GM.

4.3. **Line Managers**
4.3.1. Notify the IT Lead when staff join, leave, or change roles, triggering asset assignment or return.
4.3.2. Support the IT Lead in confirming that all issued assets are returned and cleared of sensitive data.
4.3.3. May act as owners for shared departmental assets and ensure proper usage tracking.

4.4. **Employees and Contractors**
4.4.1. Must take appropriate care of any organizational assets they receive or use.
4.4.2. Are responsible for reporting new assets, suspected damage, or misplacement immediately to the IT Lead.
4.4.3. Must not lend, share, or reassign assets without documented approval.
4.4.4. Must ensure safe storage and transport, especially for portable devices (e.g., laptops, phones, USBs).
4.4.5. Are obligated to return all assets and associated materials upon request, role change, or contract termination.

5. Governance Requirements

5.1. The IT Lead must maintain a structured asset inventory that includes the following minimum fields:
5.1.1. Asset ID or serial number
5.1.2. Asset type (e.g., laptop, phone, license)
5.1.3. Assigned owner (name and role)

5.1.4. Physical or logical location (if relevant)
5.1.5. Classification level (Internal, Confidential)
5.1.6. Status (active, pending return, retired)
5.1.7. Purchase or issuance date
5.1.8. Return or disposal date (if applicable)

5.2. All updates to the asset inventory (new entries, reassignments, removals) must be logged promptly. Spot-checks must be performed at least semi-annually to verify accuracy.

5.3. Assets must be classified according to their sensitivity or criticality. For example:
5.3.1. *Internal*: General business devices or software
5.3.2. *Confidential*: Devices storing customer data, HR records, financial information, or intellectual property

5.4. The asset inventory must be protected against unauthorized access or alteration. Access should be limited to the GM, IT Lead, and designated personnel. Backups of the inventory must be maintained.

6. Policy Implementation Requirements

6.1. **Asset Issuance and Documentation**

6.1.1. All newly purchased or reassigned assets must be recorded in the asset inventory immediately.

6.1.2. […….]

ISO/IEC 27001:2022

Clause 8.1: Requires operational controls to manage assets and protect them throughout their use.

ISO/IEC 27002:2022

Control 5.9: Details how to identify, assign ownership, classify, and manage assets securely.

NIST SP 800-53 Rev.5

CM-8: Requires organizations to develop and maintain an inventory of system components, including hardware, software, and virtual assets.

EU GDPR

Article 30: Requires documentation of data processing activities, which depends on knowing where data is stored and on what assets.

EU NIS2

Article 21(2)(a*)*: Calls for technical and organizational measures, including asset tracking, to protect network and information systems.

EU DORA

Article 5(8): Financial entities must maintain detailed inventories of ICT assets as part of ICT risk management.

COBIT 2019

BAI09: Specifies that IT assets must be managed throughout their lifecycle—from acquisition to retirement—with clear ownership and controls.