					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

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clause 8	Asset management requirements
ISO/IEC 27002:2022	Control 5	Asset management controls
NIST SP 800-53 Rev.5	CM-8	Inventory of system components
EU NIS2	Article 21(2)(a)	Asset tracking for protection of network and information systems
EU DORA	Article 5(8)	ICT asset inventory requirements
COBIT 2019	BAI	IT asset management lifecycle
EU GDPR	Article 30	Inventory of data processing activities

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 purpose 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, business continuity planning, and risk management.

1.4 This policy also supports certification to ISO/IEC 27001 and demonstrates alignment with legal, financial, and cybersecurity obligations under frameworks such as GDPR, NIS2, and DORA.

1.5 For small and medium-sized enterprises (SMEs), a simple but systematic asset management approach is essential to prevent unmanaged devices, data loss, or audit failure, particularly where technical staffing is limited.

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 working 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, smart cards, access fobs, biometric tokens

2.3 All employees, contractors, and third-party providers handling organizational assets are within the scope of this policy.

2.4 This policy also governs both short-term assets (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 and 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 to enable differentiated protection levels.

3.4 Define clear procedures for asset issuance, reassignment, maintenance, loss reporting, and retirement.

3.5 Ensure assets are handled securely 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 applicable laws (e.g., the GDPR accountability principle) and cybersecurity certification standards.

4. Roles and Responsibilities

4.1 General Manager

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 required.

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 tracking tool).

4.2.2 Assigns asset ownership and tracks changes in 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 observed (e.g., Internal, Confidential).

4.2.5 Coordinates the retrieval, sanitization, and deactivation of assets during offboarding or retirement.

4.2.6 Reports any unresolved asset discrepancies to the General Manager.

[... 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 at least annually and whenever:

9.1.1 New types of technology or assets are introduced

9.1.2 Asset tracking procedures change (e.g., through adoption of new tools or platforms)

9.1.3 New regulatory obligations affect asset traceability or disposal

9.1.4 An incident or audit identifies a gap in current asset management practices

9.2 Reviews must involve the General Manager and IT Lead and must include updates to asset handling procedures, inventory templates, and classification guidance.

9.3 All updates must be documented and communicated to affected staff. A version-controlled change log must be retained.

10. Related Policies and Linkages

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

10.2 P4S – Access Control Policy: Links asset usage (e.g., laptops, mobile devices) to user access rights and identity management.

10.3 P7S – Onboarding and Termination Policy: Ensures asset issuance and recovery are embedded in personnel lifecycle processes.

10.4 P13S – Data Classification and Labeling Policy: Provides rules for determining whether an asset should be classified as Internal or Confidential.

10.5 P30S – Incident Response Policy: Defines response procedures where an asset-related event results in a security incident or personal data breach.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001

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

11.2 ISO/IEC 27002

11.2.1 Control 5.9: Specifies how to identify, assign ownership of, classify, and manage assets securely.

11.3 NIST SP 800-53 Rev.5

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

11.4 EU GDPR

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

11.5 EU NIS2

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

11.6 EU DORA

11.6.1 Article 5(8): Requires financial entities to maintain detailed inventories of ICT assets as part of ICT risk management.

11.7 COBIT 2019

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