



ASSET MANAGEMENT POLICY

Classification: **Public**

This document may be shared with interested parties outside of [Company Name]

| Version | Approved By | Owner | Date Last Updated | Review Frequency | Next Review | Comments |
|---------|-------------|-------|-------------------|------------------|-------------|----------|
| | | | | | | |

Contents

Purpose of This Document..... 2

Scope 2

Policy Statement..... 2

Responsibilities 2

Asset Identification and Classification 2

Asset Identification 2

Asset Classification 2

Asset Registers 3

Asset Lifecycle Management 3

Acquisition 3

Use and Maintenance 3

Disposal 3

Risk Assessment and Treatment 3

Training and Awareness..... 4

Monitoring and Review 4

Compliance..... 4

Appendices 4

Purpose of This Document

The purpose of this Asset Management Policy is to establish a framework for the management of all assets within [Company Name].

This policy ensures that assets are identified, recorded, classified, and managed throughout their lifecycle, in compliance with ISO/IEC 27001:2022 control 5.9.

Scope

This policy applies to all information assets, including but not limited to hardware, software, information, and network components, owned or controlled by [Company Name].

Policy Statement

[Company Name] is committed to managing its information assets effectively to ensure their confidentiality, integrity, and availability. All assets must be identified, recorded, classified, and managed according to this policy.

Responsibilities

- **Information Security Manager:** Responsible for implementing and maintaining the Asset Management Policy.
- **Asset Owners:** Responsible for the day-to-day management and protection of assigned assets.
- **Project Managers:** Ensure information security considerations are integrated into project management processes.
- **IT Department:** Maintain the asset inventory and ensure it is updated regularly.
- **All Employees:** Comply with asset management procedures and report any changes or incidents related to assets.

Asset Identification and Classification

Asset Identification

- All assets must be uniquely identified and recorded in the appropriate asset register.
- Each asset must have a unique identifier (Asset ID).

Asset Classification

- Assets must be classified based on their sensitivity, criticality, and value.

Asset Management Policy

- Classification categories are outlined in the Information Security Policy.

Asset Registers

[Company Name] maintains multiple asset registers, each capturing key information about different types of assets.

The following registers are used:

| Asset Register | Managed by | Tool | Contains | Key Information |
|----------------------------|------------------------------|--|---|---|
| Hardware Asset Register | IT Department | Asset Inventory Management Tool (e.g., Active Directory) | Laptops, desktops, servers, network devices, etc. | Asset ID, type, description, owner, location, status, acquisition date, disposal date, classification |
| Software Asset Register | Software Asset Manager | Software Asset Management System | Operating systems, applications, licenses, etc. | Asset ID, name, version, owner, license information, status, classification |
| Information Asset Register | Information Security Manager | Document Management System | Databases, documents, intellectual property, etc. | Asset ID, title, owner, location, format, classification |

Asset Lifecycle Management

Acquisition

- All new assets must be recorded in the appropriate asset register upon acquisition.

Use and Maintenance

- Assets must be maintained and protected according to their classification and usage requirements.
- Regular audits and reviews must be conducted to ensure the accuracy of the asset registers.

Disposal

- Assets must be disposed of securely and removed from the asset register.
- Disposal methods must comply with applicable regulations and internal policies.

Risk Assessment and Treatment

- Conduct regular risk assessments to identify and address potential threats to assets.

Asset Management Policy

- Implement appropriate security controls based on the asset classification and identified risks.

Training and Awareness

- Provide training to all employees on asset management policies and procedures.
- Ensure employees are aware of their responsibilities in managing and protecting assets.

Monitoring and Review

- Conduct periodic reviews and audits of the asset registers to ensure accuracy and completeness.
- Regularly review and update this policy to reflect changes in the asset landscape and regulatory requirements.

Compliance

Non-compliance with this policy may result in disciplinary action. All employees must adhere to this policy and report any issues or incidents related to asset management.

Appendices

Appendix A: Sample Asset Register Template

| Asset ID | Asset Type | Description | Owner | Location | Status | Classification | Acquisition Date | Disposal Date | Comments |
|----------|------------|-------------------------|---------------|-------------|--------|----------------|------------------|---------------|----------|
| 001 | Laptop | Dell Latitude 7420 | John Doe | Office A123 | Active | Internal | 2023-01-15 | N/A | |
| 002 | Software | Microsoft Office 365 | Jane Smith | Cloud | Active | Public | 2022-03-10 | N/A | |
| 003 | Server | HP ProLiant DL380 Gen10 | IT Department | Data Center | Active | Confidential | 2021-08-22 | N/A | |