# ISO 27001-Compliant Asset Management Procedure Template

## Introduction

This Asset Management Procedure aligns with ISO 27001 standards, providing a structured framework for identifying, classifying, and managing organizational assets to ensure their protection throughout their lifecycle. This procedure supports the confidentiality, integrity, and availability of information assets critical to business operations.

## Purpose

The purpose of this procedure is to define a systematic approach to managing assets, including their identification, ownership, classification, and protection. This ensures that all organizational assets are accounted for and adequately safeguarded against risks, aligning with legal, regulatory, and business requirements.

## Scope

This procedure applies to all organizational assets, including:

* Physical assets such as servers, workstations, and mobile devices
* Information assets, including databases, documents, and intellectual property
* Software assets, such as applications and licenses
* Human assets, including employees and contractors with access to critical systems
* Third-party assets, including outsourced services and cloud-based solutions

## Policy Statement

The organization is committed to implementing a robust asset management framework that ensures:

* Identification and inventory of all assets
* Assignment of ownership for accountability
* Classification of assets based on criticality and sensitivity
* Implementation of controls to protect assets from unauthorized access, use, or modification
* Regular review and update of asset records

The procedure includes the following six steps:

1. Asset Identification: Create and maintain an inventory of all assets, capturing key details such as type, location, owner, and value.
2. Ownership Assignment: Designate responsible owners for each asset to ensure accountability for its management and protection.
3. Classification: Classify assets based on their criticality, sensitivity, and value to the organization.
4. Protection: Implement appropriate controls, including access restrictions, encryption, and physical security measures.
5. Monitoring and Auditing: Regularly review asset inventories and conduct audits to ensure compliance with policies and standards.
6. Decommissioning: Establish procedures for securely disposing of or repurposing assets at the end of their lifecycle.

## Roles and Responsibilities

* Asset Manager: Maintains the asset inventory and oversees classification and protection measures.
* Information Security Officer: Ensures asset management practices align with ISO 27001 requirements.
* IT Operations Team: Implements technical controls for the protection and monitoring of assets.
* Department Heads: Ensure assets within their areas are accounted for and managed according to this procedure.
* Third-Party Vendors: Comply with organizational requirements for managing outsourced or shared assets.

## Compliance and Monitoring

Compliance with this procedure will be ensured through:

* Regular updates to the asset inventory
* Periodic audits and inspections of asset management practices
* Key performance indicators (KPIs), such as:

- Percentage of assets with assigned ownership

- Frequency of asset inventory updates

- Number of non-compliance findings during audits

The effectiveness of the asset management program will be evaluated by benchmarking against industry standards and incorporating feedback from audits and incidents.

## Related Documentation

* Information Security Policy
* Risk Assessment Procedure
* Access Control Policy
* Incident Response Plan

## Review and Revision

This procedure will be reviewed annually or when significant changes occur in the organizational environment or regulatory requirements. The Asset Manager will initiate the review process, and updates will be communicated to stakeholders through official channels. All updates will be documented and approved through a formal review process.

## Narrative Guidance

This procedure emphasizes the importance of comprehensive asset management in maintaining organizational security. It aligns with ISO 27001 principles of accountability, risk management, and continuous improvement. Organizations are encouraged to adapt this template to meet their specific operational and regulatory needs.

## Instructions for Use

* Replace placeholders with organization-specific details.
* Ensure alignment with related policies and standards.
* Collaborate with stakeholders to address unique organizational risks and objectives.