# ISO 27001 Asset Management Lifecycle Template

## Introduction:

This document outlines the Asset Management Lifecycle Process for [COMPANY NAME], aligned with ISO 27001 requirements. It ensures that information assets are identified, classified, managed, and protected throughout their lifecycle. The process integrates with the Information Security Management System (ISMS) to safeguard the confidentiality, integrity, and availability of information assets.

## 1. Purpose of the Asset Management Lifecycle

The purpose of this process is to:  
1. Identify and classify information assets critical to the organization.  
2. Manage assets throughout their lifecycle, from acquisition to decommissioning.  
3. Protect assets against unauthorized access, misuse, and vulnerabilities.  
4. Ensure compliance with legal, regulatory, and contractual obligations related to asset management.  
5. Support risk management and align with ISO 27001 controls.

## 2. Asset Management Lifecycle Stages

The asset management lifecycle involves the following stages. Refer to the lifecycle diagram below for a visual representation.

* Acquisition: Define asset requirements, conduct risk assessments, and ensure secure procurement.
* Registration: Record assets in the Asset Register, assign unique identifiers, and capture essential details.
* Classification: Classify assets based on criticality and sensitivity. Assign security controls accordingly.
* Usage and Maintenance: Define guidelines for use, ensure regular maintenance, and monitor performance.
* Monitoring: Track assets for unauthorized access, vulnerabilities, and changes in status.
* Decommissioning and Disposal: Safely remove assets from service, ensuring secure data destruction.

Lifecycle Diagram:  
(Insert a graphical representation of the lifecycle here.)

## 3. Asset Categories

* 1. Hardware: Physical devices such as laptops, servers, and network equipment.
* 2. Software: Licensed software, applications, and operating systems.
* 3. Data: Information stored in databases, files, and systems.
* 4. Personnel: Individuals with access to sensitive information or critical systems.
* 5. Third-Party Assets: Vendor-provided equipment or cloud-hosted services.

## 4. Risk Integration

Each asset should undergo a risk assessment to identify potential threats, vulnerabilities, and impacts. Mitigation strategies and controls should be applied based on the risk assessment results.

## 5. Asset Register Template

Use the table below as a template to document and track assets:

| Asset ID | Asset Name | Owner | Classification | Location | Status | Acquisition Date | Disposal Date |
| --- | --- | --- | --- | --- | --- | --- | --- |

## 6. Metrics for Asset Management

* Percentage of assets classified and registered in the Asset Register.
* Number of incidents related to asset misuse or unauthorized access.
* Average time to detect and remediate vulnerabilities in critical assets.
* Percentage of assets securely decommissioned within the defined timeframe.

## 7. Roles and Responsibilities

Asset Owner:  
- Maintain the accuracy of asset details.  
- Ensure assets are used and protected per policies.

Information Security Manager (ISM):  
- Oversee classification and control implementation.  
- Conduct regular audits of the Asset Register.

IT Operations Team:  
- Implement and monitor technical controls.  
- Address vulnerabilities and maintain asset performance.

Compliance Officer:  
- Ensure alignment with regulatory and contractual requirements.

Employees and Contractors:  
- Use assets responsibly and report any incidents.

## 8. Revision and Maintenance

This document and the Asset Management Lifecycle Process will be reviewed [Insert frequency, e.g., annually or as needed] to ensure it remains aligned with organizational priorities, regulatory requirements, and the threat landscape.

## Approval:

| Name | Title | Date |
| --- | --- | --- |
|  |  |  |
|  |  |  |