Company Name

policy Name

**REVISION HISTORY**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Version | Date | Author | Reviewer | Approver | Description Of Changes |
| 1.0 | 22/03/2024 | Name | Name | Name | First release |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**INDEX**

[1. Purpose: 3](#_Toc185944263)

[2. Scope: 3](#_Toc185944264)

[3. Definitions: 3](#_Toc185944265)

[4. Roles and Responsibilities: 4](#_Toc185944266)

[5. Policy Statements: 4](#_Toc185944267)

[5.1 Acquisition of IT Assets: 4](#_Toc185944268)

[5.2 Asset Classification 4](#_Toc185944269)

[5.3 Inventory and Asset Register 4](#_Toc185944270)

[5.4 Asset Ownership 5](#_Toc185944271)

[5.5 Acceptable Use of Assets: 5](#_Toc185944272)

[5.6 Removable Media and Data Transfers 5](#_Toc185944273)

[5.7 Return of Assets: 6](#_Toc185944274)

[5.8 Disposal of Assets 6](#_Toc185944275)

[5.9 Licensing and Software Compliance: 6](#_Toc185944276)

[5.10 Reporting Lost or Stolen Assets: 6](#_Toc185944277)

[6. Compliance: 6](#_Toc185944278)

[7. Policy Review and Improvements: 7](#_Toc185944279)

## Purpose:

The purpose of this Asset Management Policy is to ensure that all assets within ABC are properly identified, classified, maintained, and protected throughout their lifecycle. This policy aims to ensure efficient use of resources, protect information, and reduce security risks, aligning with ISO 27001:2022 standards.

## Scope:

This policy applies to all **information and technology assets** managed by ABC, covering both **physical and digital forms** across all stages of their lifecycle—from acquisition through disposal. Assets covered under this policy include, but are not limited to:

* **IT systems and applications** (e.g., software, databases)
* **Physical assets** (e.g., laptops, servers, desktops)
* **Data assets** (e.g., client data, intellectual property, HR records)
* **Mobile devices** (e.g., smartphones, tablets)
* **Network infrastructure** (e.g., routers, switches, firewalls)
* **Services** (e.g., cloud services, internet services)

This policy applies to **all employees, contractors, and third-party vendors** who have access to or manage ABC’s assets, ensuring they adhere to requirements for **asset protection, usage, maintenance, and disposal** in alignment with ABC’s security standards.

## Definitions:

1. **Asset**: Any physical, digital, or information-based resource that is owned or controlled by ABC.
2. **Asset Lifecycle**: The phases through which an asset passes, including acquisition, usage, maintenance, and disposal.
3. **Asset Owner**: The individual or department responsible for overseeing the use, security, and lifecycle management of an asset.
4. **Asset Custodian**: The individual responsible for the day-to-day management and security of an asset.
5. **Asset Register**: A comprehensive inventory of all assets, including their classification, location, and ownership.

## Roles and Responsibilities:

* **Director**: Responsible for overseeing the implementation and compliance of this policy.
* **Information Security Officer (ISO)**: Ensures compliance with this policy, conducts periodic audits, reports non compliances and periodically review the classification levels and associated controls
* **IT Manager**: Implements the technical controls for asset management, maintains the **Asset Register**, and ensures assets are classified and protected.
* **HR Department**: Collaborates with IT during employee onboarding and offboarding to ensure timely provisioning and de-provisioning of assets.
* **All Employees**: Must comply with the Asset Management Policy, use assets responsibly, and report any loss, damage, or theft immediately.

## Policy Statements:

### Acquisition of IT Assets:

1. Assets shall be procured through approved processes including market surveys, purchase requests, and management approvals.
2. Assets should be properly assessed/ inspected before installation in ABC’s network/ premises.

### Asset Classification

1. **All assets shall be classified based on their sensitivity and criticality**. Each classification level dictates specific handling protocols, including access permissions, encryption, and retention requirements, to ensure data is protected in accordance with confidentiality needs

* **Public**: Information that can be freely shared with the public. Accessible without restriction; no confidentiality requirements.
* **Internal**: Information accessible only to ABC employees. Restricted to authorized personnel, with minimal handling controls.
* **Confidential**: Sensitive information requiring strict controls, including encryption and restricted access to authorized personnel only, due to its sensitive nature.

### Inventory and Asset Register

1. IT Manager is responsible for maintaining an up-to-date Asset Register that includes:
   1. **Type of asset** (e.g., physical, software, information)
   2. **Location**
   3. **Owner and custodian**
   4. **Classification** (e.g., Public, Internal, Confidential)
   5. **Status** (e.g., in use, under maintenance, retired)
2. Quarterly reviews and audits of the Asset Register shall be conducted to ensure accuracy and ensure security controls are applied as necessary.
3. Quarterly reviews of the Asset Register shall also include an audit of asset classification levels. Reclassification should occur if asset sensitivity or business requirements change, ensuring continued alignment with security policies.

### Asset Ownership

1. Every asset must have an Asset Owner who is responsible for:

* Ensuring that the asset is used correctly and securely.
* Maintaining the asset throughout its lifecycle.
* Updating the IT team with any changes in status (e.g., disposal, reassignment).

1. The Asset Custodian is responsible for the day-to-day handling, use, and maintenance of the asset.

### Acceptable Use of Assets:

1. All employees must use ABC's assets responsibly, ensuring:
2. All employees must use ABC's assets responsibly, ensuring:
3. Only authorized software is installed.
4. Downloading unauthorized content, including personal files or unapproved applications, is prohibited.
5. Access to prohibited websites is restricted, and assets should not be used for personal or non-business activities.
6. Computers and devices are logged off or shut down when not in use.
7. Antivirus and other security software shall not be disabled or modified.

### Removable Media and Data Transfers

1. Use of removable media (e.g., USB drives, external hard drives) is restricted and shall be approved by the IT Manager.
2. All data transferred via removable media shall be encrypted.
3. Periodic reviews of removable media usage shall be conducted to ensure compliance with security requirements.
4. Confidential data on removable media must be encrypted, and usage shall be logged and periodically reviewed. Unauthorized usage of removable media is strictly prohibited.

### Return of Assets:

1. Upon termination of employment or completion of contracts, all assets shall be returned to the IT Manager.
2. When replacing old assets with new ones, the old assets must be returned, and the Asset Register updated to reflect the new asset status.

### Disposal of Assets

1. Assets that are no longer in use shall be securely disposed of to prevent unauthorized access or recovery of sensitive data.
2. Data on all hardware (e.g., laptops, servers) must be permanently erased using approved methods before disposal.
3. The IT Manager shall approve any removal of assets from ABC premises for repairs, servicing, or replacement.
4. Data on Confidential assets must be permanently erased using approved erasure tools. Physical assets, such as drives or printed materials, must be disposed of through certified destruction services, documented in the Asset Register.

### Licensing and Software Compliance:

1. IT Manager shall be responsible for maintaining software licenses and ensuring compliance with license agreements.
2. Employees must not install any unauthorized software, and all software shall be used in accordance with the applicable licensing terms.

### Reporting Lost or Stolen Assets:

1. Any lost or stolen assets shall be reported to the IT Manager immediately.
2. The IT Manager will investigate the incident, disable the asset, and ensure appropriate measures are taken to protect data.

## Compliance:

Compliance with this policy is mandatory. Breaches of this policy may result in disciplinary action and could lead to the termination of employment or contracts.

## Policy Review and Improvements:

This policy will be reviewed annually or in response to significant changes to the ISMS, operational practices, or after any security incidents, to ensure its continuing suitability, adequacy, and effectiveness.