Asset Management Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

ABC Company is committed to protecting its Staff, customers, partners and its operations. This policy enables ABC Company to effectively deliver equipment and services that support company business processes.

# II. Purpose

This policy protects ABC Company’s assets and helps ensure our ability to continue business operations.

# III. Scope

This policy applies to all ABC Company Staff that have access to ABC Company’s Information Resources.

# IV. Policy

A. Asset Types

The following types of devices shall be tracked assuming they meet the other requirements of this policy:

* Desktop workstations
* Firewalls
* Handheld devices
* Laptop mobile computers
* Memory devices
* Printers, Copiers, FAX machines, multifunction machines
* Routers
* Scanners
* Servers
* Software (application and operating system)
* Switches

B. Asset Value

Assets which cost less than $100 shall not be tracked specifically including computer components such as video cards or sound cards. However, assets which store data regardless of cost shall be tracked. These assets include:

* Hard Drives
* Temporary storage drives
* Tapes with data stored on them including system backup data

Although not specifically tracked, other storage devices including CD ROM disks and USB flash drives are covered by this policy for disposal and secure storage purposes.

C. Asset Media

Small memory storage assets will not be tracked by location. Instead, they will be tracked and inventoried by Data Owner. Enterprise software should be used that can configure systems to allow the use of small storage devices on specific Information Systems. These assets include:

* CD/DVD disks
* Memory sticks (USB flash drives)

If these types of devices are permitted for some Staff, the Data Owner of the device must sign for receipt of these devices in their possession. All Staff must also agree to handle memory sticks, and CD/DVD disks in a responsible manner and follow these guidelines:

* Never place sensitive data on them without authorization. If sensitive data is placed on them, special permission must be obtained and the memory device must be kept in a secure area.
* Never use these devices to bring executable programs from outside the network without authorization and without first scanning the program with an approved and updated anti-virus and malware scanner. Any program brought into the network should be on the IT department list of approved programs.
* The Memory Device Data Owner agreement allows Staff to sign for receipt of these devices and agree to handle these devices in accordance with the terms of this policy. This form must be submitted by all Staff that will work with any organizational data when the Staff begins working for the organization. It will also be submitted when Staff receives one or more memory sticks, temporary storage drives, or data backup drives.

D. Asset Tracking Requirements

All assets must have an ID number. Either an internal tracking number will be assigned when the asset is acquired or the use of Manufacturer ID numbers must be specified in this policy.

An asset tracking database (Database) shall be created to track assets. It will include all information on the Asset Transfer Form including the date of the asset change.

The Database shall be maintained, accurate, and kept up-to-date. The Database shall include an inventory of all Information System assets that have the potential to store or process information. The inventory shall include all hardware and software assets, whether connected to the organization's network or not. Any unauthorized assets shall be removed, quarantined, or the inventory updated in a timely manner. When an asset is acquired, an ID will be assigned for the asset and its information shall be entered in the Database. All assets maintained in the Database inventory must have an assigned owner.

Software applications and operating systems currently supported and receiving vendor updates shall be added to the Database. Unsupported software shall either be removed or classified as Unsupported in the Database.

E. Transfer Procedure

Asset Transfer Checklist - When an asset type listed on the Asset Types list is transferred to a new location or Data Owner, the IT Asset Transfer Checklist must be filled out by the Data Owner of the item and approved by an authorized representative of the organization. The Data Owner is the person responsible for the asset. If the item is a workstation, then the Data Owner is the most common user of the workstation. For other equipment, the Data Owner is the primary person responsible for maintenance or supervision of the equipment.

The Data Owner must fill out the Asset Transfer Checklist form and indicate whether the asset is a new asset, moving to a new location, being transferred to a new Data Owner, or being disposed. The following information must be filled in:

* Asset Type
* ID number
* Asset Name
* Asset Description
* Current Location
* Designated Data Owner
* New Location
* New Data Owner
* Locations of Sensitive Data

Approval - Once the Data Owner fills out and signs the Asset Transfer Checklist form an authorized representative must sign it.

Data entry - After the Asset Transfer Checklist is completed, it will be given to the Database manager. The asset tracking Database manager shall ensure that the information from the forms is entered into the Database within one week.

Database - An active discovery tool shall be used to identify devices connected to the network. Software inventory tools shall be used to identify and classify operating system and application software on such devices. The Database shall be updated based upon the results of the hardware and software inventory tools. Where possible, the Database shall be automatically updated through the use of automated tools. Resource Owners shall check the Database on a regular basis to ensure applicable assets are included in the Database.

F. Asset Transfers

This policy applies to any asset transfers including the following:

* Asset purchase
* Asset relocation
* Change of asset Data Owner including when Staff leaves or is replaced
* Asset disposal
* In all these cases the asset transfer checklist must be completed

G. Asset Disposal and Repurposing

Procedures governing asset management shall be established for secure disposal or repurposing of equipment and resources prior to tenant assignment or jurisdictional transport.

Asset disposal is a special case since the asset must have any sensitive data removed prior to disposal. The manager of the user of the asset shall determine the level of maximum sensitivity of data stored on the device.

Below is listed the action for the device based on data sensitivity according to the data classification process:

* Public - No requirement to erase data but in the interest of prudence normally erase the data using any means such as reformatting or degaussing
* Sensitive - Erase the data using any means such as reformatting or degaussing
* Confidential - The data must be erased using an approved technology to make sure it is not readable using special technology techniques approved by the Chief Security Officer.

H. Media Use

This policy defines the types of data that may be stored on removable media and whether that media may be removed from a physically secure facility and under what conditions it would be permitted. Removable media includes:

* Memory stick/flash drive
* CD/DVD disk
* Storage tape

Below is listed the policy for the device based on the rated data sensitivity of data stored on the device according to the data classification process:

* Public - Data may be removed with approval of the first level manager and the permission is perpetual for the Staff duration of employment unless revoked. The device may be sent to other offices using any public or private mail carrier.
* Sensitive - Data may only be removed from secure areas with the permission of a director level or higher level of management and approvals are good for one time only.
* Confidential - The data may only be removed from secure areas with permission of a Vice President or higher level of management. Staff shall document security precautions for both the transport method and at the destination.

I. Separation of Duties

Duties and job functions shall be separated to ensure Information Resource availability, confidentiality, and integrity.

J. Clearing and Sanitation

Clearing is the process of eradicating the data on media before reusing the media in an environment that provides an acceptable level of protection for the data that was on the media before clearing. All internal memory, buffer, or other reusable memory shall be cleared to effectively deny access to previously stored information.

Sanitization is the process of removing the data from media before reusing the media in an environment that does not provide an acceptable level of protection for the data that was in the media before sanitizing. Information Resources shall be sanitized before they are released from Sensitive Information controls or released for use at a lower classification level. Overwriting is no longer acceptable for sanitization of magnetic media. Only degaussing or physical destruction is acceptable.

K. Protection Measures

Protection profiles required for a particular information system shall be determined by the Level of Concern for Confidentiality and by the operating environment of the system as reflected by the clearances, access approvals, and need-to-know.

Procedures shall ensure that the proper access and integrity controls prevent the improper alteration or destruction of data.

A transaction log, protected from unauthorized changes, shall document:

* The off-line verification of all changes
* The immediate correction of unauthorized data and Information System software changes

Procedures shall be implemented that:

* Define logical access controls where the security support structure defines and controls access between named users and named objects (e.g., files and programs) in the system
* Support this policy and its security mechanisms
* Define processes or mechanisms that allow users (or processes acting on their behalf) to determine the formal access approvals granted to another user
* Define processes or mechanisms that allows users (or processes acting on their behalf) to determine the sensitivity level of data

The Information System shall provide a protected capability to control the number of logon sessions for each user ID, account, or specific entry point. The default shall be a single logon session.

The Information System shall detect an interval of user inactivity, such as no keyboard entries, and shall disable any future user activity until the user re-establishes the correct identity with a valid authenticator. The inactivity time period and restart requirements shall be documented in the Securing Information Systems Policy.

If the operating system provides the capability, the user shall be notified upon successful logon of: the date and time of the user’s last logon; the location of the user (as can best be determined) at last logon; and the number of unsuccessful logon attempts using this user ID since the last successful logon. This notice shall require positive action by the user to remove the notice from the screen.

# V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This policy is to be distributed to all ABC Company Staff.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT APO01.06, APO09.03, BAI09.01, BAI09.02-03, DSS04.07, DSS05.04-05, DSS06.06

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(B)

ISO 27001 A.8, A.9

NIST SP 800-37 3.1, 3.3

NIST SP 800-53 CM-8, PL-4

NIST Cybersecurity Framework ID.AM, PR.PT, DE.DP-2, DE.CM-1-2, RS.RP-1

PCI 1.1.5