Asset Management Policy

Summary

This Asset Management Policy establishes comprehensive guidelines for the inventory, control, and protection of organizational assets within our organization. It outlines procedures for asset classification, inventory management, ownership, acceptable use, return processes, media handling, disposal, and compliance monitoring. The policy aims to ensure the efficient use, protection, and accountability of all organizational assets throughout their lifecycle.

Purpose

The purpose of this Asset Management Policy is to: Establish a systematic approach to managing organizational assets Ensure the protection and optimal utilization of assets Maintain accurate records of all assets and their ownership Define acceptable use guidelines for organizational assets Outline procedures for the secure handling and disposal of assets Ensure compliance with relevant laws, regulations, and organizational standards

Scope

This policy applies to:

- All employees, contractors, and third-party users
- All organizational assets, including but not limited to:
    - Physical assets (e.g., computers, mobile devices, furniture)
    - Information assets (e.g., databases, documents, intellectual property)
    - Software assets (e.g., applications, licenses)
    - Network assets (e.g., servers, routers, switches)
- All departments and locations within the organization

Definitions

Term	**Definition**
Asset	Any item of value to the organization, including physical, information, software, and network resources
Asset Owner	The individual or department responsible for the management, control, and maintenance of an asset

Term	Definition
Asset Register	A centralized inventory of all organizational assets, including their details and current status
Media	Any device or material used to store and transmit information, including physical and digital formats
Disposal	The process of securely removing an asset from organizational use and ownership

Policy Section

Asset Classification

All assets must be classified according to their criticality and sensitivity. Classification levels shall include Critical, Sensitive, Internal, and Public. Asset classification must be reviewed annually or when significant changes occur.

Asset Inventory Management

An up-to-date asset register must be maintained, including unique asset identifier, asset description, classification, owner, location, purchase date and cost, and maintenance schedule. Regular audits of the asset register must be conducted at least annually. Any discrepancies in the asset register must be investigated and resolved promptly.

Asset Ownership

Each asset must have a designated owner responsible for ensuring appropriate use and protection of the asset, periodic review of access rights, and approving changes to the asset's classification or status. Asset ownership must be clearly documented in the asset register. Changes in asset ownership must be formally recorded and approved.

Acceptable Use of Assets

All users must comply with the organization's Acceptable Use Policy. Assets must only be used for authorized business purposes, and users are responsible for the protection of assets assigned to them. Remote access to organizational assets must be in accordance with the Remote Access Policy.

Asset Return Process

All assets must be returned to the organization upon termination of employment or contract. A formal asset return process must be followed, including verification of returned assets against the asset register, assessment of asset condition, and updating the asset register accordingly. Any discrepancies in returned assets must be reported to management immediately.

Media Handling

All media containing sensitive or critical information must be securely stored when not in use. Transmission of sensitive information must be encrypted. Removal of media containing organizational data from premises must be authorized, and a log of media movements must be maintained.

Asset Disposal

All assets must be disposed of securely and in compliance with environmental regulations. Electronic devices and media must undergo secure data wiping before disposal. Disposal of assets must be documented and recorded in the asset register. Third-party disposal services must be vetted and contractually bound to follow organizational security requirements.

Compliance Monitoring

Regular compliance audits must be conducted to ensure adherence to this policy. Non-compliance must be reported to management and addressed promptly. Policy effectiveness must be reviewed annually and updated as necessary. All employees must acknowledge their understanding and compliance with this policy annually.

Enforcement

Violations of this policy may result in disciplinary action, up to and including termination of employment. The severity of the disciplinary action will be determined based on the nature and impact of the violation. All employees are required to report suspected violations to their immediate supervisor or the Information Security team. The organization reserves the right to report illegal activities to appropriate law enforcement authorities.

Roles and Responsibilities

Role	**Description**
Chief Information Security Officer (CISO)	Oversees the implementation and maintenance of the information security program, including this policy.

Role	Description
Information Security Team	Develops, implements, and monitors security controls, conducts risk assessments, and provides guidance on security matters.
IT Department	Implements technical controls, manages system configurations, and assists in incident response.
Human Resources	Ensures employees receive security awareness training and handles disciplinary actions related to policy violations.
Legal Department	Provides guidance on legal and regulatory compliance aspects of information security.
All Employees	Adhere to this policy, report security incidents, and participate in security awareness training.

Control Mapping

Framework	Control ID	Description
HIPAA	164.308	Administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures
HIPAA	164.310	Physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment
HIPAA	164.312	Technology and related policies and procedures that protect ePHI and control access to it

Framework	Control ID	Description
HIPAA	164.316(a)	Implement reasonable and appropriate policies and procedures
HIPAA	164.316(b)(1)	Maintain documentation of required policies and procedures
HIPAA	164.414	Requirements for maintaining documentation and records

Revision History

Version	Date	Author	Changes

Approval

Name	Title	Date	Signature