Asset Management Policy

Purpose

The purpose of this policy is to outline guidelines and practices to protect IT assets used to access sensitive customer or company data, and ensure any such access maintains the security and confidentiality of the data.

Scope

This policy applies to <Company Name>'s physical IT assets, such as laptops, tablets, and smartphones, and all employees and contractors that use them. It also applies to employee-owned devices used to access company information.

Ownership

[POLICY OWNER]

is responsible for implementing and maintaining this policy.

Policy Statement

Inventory

The company maintains an inventory of IT infrastructure devices.

Maintaining a complete asset inventory is necessary for keeping IT assets and the data they access and process secure. While <Company Name> considers its employees' workstations its most critical physical assets to inventory, it may additionally track other asset types, such as company-provided mobile devices or networking office equipment. [POLICY OWNER]

is responsible for maintaining an inventory of these assets using automated or manual means.

Each asset in the inventory is assigned an owner, typically representing its primary user. The asset owner is responsible for complying with relevant sections of the Acceptable Use and Asset Management policies. If an asset is reassigned to another employee, the asset's ownership record should be updated to reflect this change.

Company-owned IT assets which do not process or access customer data, such as printers or scanners, have no impact on data security and as such may be excluded from the inventory.

Workstations - OS

The company monitors the IT infrastructure devices for compliance with the Asset Management Policy and checks for requirements such as hard drive encryption, user authentication requirements, and security patching.

<Company Name> leverages a monitoring tool to ensure IT assets are secure and compliant. The tool can either actively manage and enforce compliance at the endpoint, passively report an endpoint's compliance status, or disallow endpoint access from non-compliant devices.

Requirements monitored include data and settings such as:

Full disk encryption status
Operating system-level firewall configuration
Biometric and strong password enforcement
Current operating system version