

Asset Management Policy

Purpose

Your Organization cannot protect what it does not know it has. This policy establishes how Your Organization identifies, inventories, classifies, and tracks its information assets — hardware, software, and the data they hold — across their lifecycle, so that every other security control (access, patching, monitoring, disposal) can be applied consistently and completely.

Scope

This policy applies to all assets owned, leased, or managed by Your Organization that store, process, or transmit company or customer data, including servers, endpoints, mobile devices, network equipment, cloud resources, SaaS accounts, and the software and licenses installed on them. It applies to IT Operations, Engineering, and any team that provisions or retires assets.

Asset inventory

- Your Organization maintains a current inventory of hardware assets (servers, endpoints, network devices, mobile devices) and software assets (applications, cloud services, licenses) that touch company or customer data.
- Each inventory record includes, at minimum: a unique identifier, asset type, owner, location or hosting environment, criticality/data classification it handles, and lifecycle status (provisioned, in service, decommissioned).
- Cloud and SaaS assets are captured via automated discovery where tooling supports it, supplemented by procurement and IT onboarding records for services outside automated reach.
- The inventory is reconciled against authoritative sources (MDM, cloud provider APIs, identity provider) on a recurring schedule to catch drift and shadow IT.

Asset ownership

Every asset has a named owner accountable for its security posture — patching, configuration, access review, and eventual decommissioning. Ownership is recorded in the inventory and transferred formally when responsibility changes teams.

Lifecycle management

Acquisition and provisioning

New hardware and software must be acquired through Your Organization-approved procurement channels and provisioned from an approved baseline configuration (see the Configuration Management Policy) before being

placed into service.

In-service management

Assets are kept current with vendor security patches, monitored per the applicable security tooling, and included in periodic vulnerability scanning. Asset criticality and data classification are reassessed when the asset's role changes.

Decommissioning

When an asset reaches end of life or end of use, it is removed from active service, its data is sanitized or securely destroyed per the Data Retention Policy, associated accounts and credentials are revoked, and the inventory record is updated to reflect decommissioned status. Decommissioning is tracked to completion, not just initiated.

Unauthorized and unmanaged assets

Assets discovered that are not in the authoritative inventory (shadow IT, unmanaged cloud resources, personally owned devices touching company data) are investigated, brought under management or removed, and the root cause of the gap addressed.

Software and license management

Your Organization tracks software licenses to avoid both compliance exposure (unlicensed use) and unnecessary spend (unused licenses), and to ensure that only approved, supported software versions remain in use.

Roles and responsibilities

- **IT Operations.** Maintains the authoritative asset inventory, discovery tooling, and decommissioning process.
- **Asset Owners.** Keep their assigned assets patched, correctly configured, and accurately reflected in the inventory.
- **Procurement.** Ensures new hardware and software purchases are routed through IT for inventory intake before deployment.
- **Information Security.** Reviews the inventory for coverage gaps and incorporates it into risk assessments and vulnerability management.

Review cadence

This policy is reviewed annually by IT Operations and Information Security, or sooner following a significant change in Your Organization's infrastructure footprint or hosting model.

Effective date: [the date this policy takes effect]