Cybersecurity Policy Templates

Asset Management Policy

(Last Updated April 2025)

Purpose

Our Asset Management Policy aims to establish a systematic and up-to-date inventory of all information technology assets within our organization, ensuring their proper management, monitoring, and protection. This policy provides clear guidelines and procedures for identifying, documenting, and tracking hardware, software, network devices, and other digital assets throughout their lifecycle. By implementing effective Asset Management practices, this policy seeks to enhance our visibility and understanding of our technology landscape, improve asset management, and strengthen cybersecurity controls. Through regular asset audits, vulnerability assessments, and risk assessments, we strive to identify and mitigate potential vulnerabilities, ensure timely patching and updates, and protect our systems, data, and networks from unauthorized access and potential threats. By prioritizing Asset Management, we enhance our overall cybersecurity posture, enable effective risk management, and maintain our critical assets' integrity, confidentiality, and availability.

Scope

The Asset Management Policy applies to all our organization's employees, contractors, and stakeholders and encompasses the systematic identification, tracking, and management of all information technology assets within our infrastructure. This policy covers hardware devices, software applications, network components, and data repositories. It establishes procedures for conducting regular asset inventories, maintaining accurate asset ownership and location records, and updating the inventory as new assets are acquired or retired. The policy sets forth guidelines for asset discovery and monitoring techniques to identify unauthorized or unmanaged assets within the organization's network. Compliance with this policy is mandatory for all individuals within the organization, and any deviations or exceptions require approval from the designated authority responsible for asset inventory and cybersecurity governance.

Safeguards

To achieve the organization's overall mission, and the purpose of this cybersecurity policy, the organization shall:

AST-01	Maintain one centralized information system asset inventory tracking system to track each of the organization's logical computing information systems.
AST-02	Ensure the organization's asset tracking system includes all endpoint computing devices (such as workstations or laptops), whether onsite or remote.
AST-03	Ensure that the organization's asset tracking system includes all server computing devices (such as physical or virtualized server instances), whether onsite or remote.
AST-04	Ensure the organization's asset tracking system includes all mobile computing devices (such as phones and tablets), whether onsite or remote.
AST-05	Ensure that the organization's asset tracking system records essential technical information about each information asset (including name, hardware address, and network address).
AST-06	Ensure that the organization's asset tracking system records essential business information about each information asset (including business owner, criticality, business unit, and approvals).
AST-07	Maintain an automated asset discovery platform to discover information assets (actively or passively) to ensure the organization's asset tracking system is accurate and automatically updated regularly.
AST-08	Define a process the organization shall use to approve each information asset in the organization's asset tracking system.
AST-09	Define a process the organization shall use to remove unauthorized information assets from the organization's network and decommission unauthorized assets.

Policy Sanctions

Non-compliance with this policy may result in disciplinary action in line with our corporation's human resources procedures. Consequences may range from mandatory refresher training and written warnings to temporary suspension of remote access privileges and, in severe cases, termination of employment or contractual obligations. Individuals could be subject to legal consequences under applicable laws if violations involve illegal activities. These sanctions emphasize the critical importance of cybersecurity, the individual's role in protecting our digital assets, and the potential risks associated with policy violations. Enforcement will be consistent and impartial, with the severity of the action corresponding directly to the seriousness of the breach.