Cybersecurity
Policy Templates

Software Management Policy

(Last Updated April 2025)

Purpose

Our Software Management Policy aims to establish a comprehensive framework for identifying, tracking, and managing software assets within our organization, ensuring their security, compliance, and effective lifecycle management. This policy provides clear guidelines and procedures for discovering, cataloging, and maintaining an accurate inventory of software applications and systems across our network. By implementing effective software inventory and discovery practices, this policy seeks to enhance visibility into our software landscape, improve license compliance, identify and remediate vulnerabilities, and reduce the risk of unauthorized or unsupported software deployments. Through regular software audits, vulnerability assessments, and patch management, we strive to mitigate the potential security risks associated with unapproved or outdated software, protect against software-related vulnerabilities, and maintain the integrity, confidentiality, and availability of our systems and data. By prioritizing software inventory and discovery, we enable effective software asset management, strengthen our overall cybersecurity posture, and ensure regulatory compliance.

Scope

The Software Management Policy applies to all our organization's employees, contractors, and stakeholders. It encompasses systematically identifying, tracking, and managing all software applications and licenses utilized within our infrastructure. This policy covers commercial and in-house-developed software, including operating systems, productivity tools, and specialized applications. It establishes procedures for conducting regular software inventories, maintaining accurate records of software installations and versions, and tracking software licenses to ensure compliance. The policy sets forth guidelines for software discovery and monitoring techniques to identify unauthorized or unmanaged software 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 software inventory and cybersecurity governance.

Safeguards

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

SW-01 Maintain a system to maintain an inventory of the organization's approved software.

SW-02 Ensure the organization's software inventory system records appropriate demographics for each software application.

SW-03 Ensure the organization's software inventory system regularly updates the software inventory via an automated discovery tool.

SW-04 Ensure the organization's software inventory system correlates the organization's hardware and software inventories in the same system.

SW-05 Ensure the organization's software inventory system validates that all software in the inventory is still supported by the software vendor.

SW-06 Ensure the organization's software inventory system validates that all operating system software in the organization's software inventory is kept up to date.

SW-07 Ensure the organization's software inventory system validates that all application software in the organization's software inventory is kept up to date.

SW-08 Maintain a Service Level Agreement (SLA) for the organization to define how often software updates must be performed on each software application.

SW-09 Define a process the organization shall use to ensure all software adheres to the organization's approved software-update Service Level Agreement (SLA).

SW-10 Maintain a software application control system on each organization's computing systems to ensure that only authorized software can execute.

SW-11 Ensure the organization's application control system only allows the execution of authorized binaries on each of the organization's computing systems.

SW-12 Ensure the organization's application control system only allows authorized software libraries (such as DLLs) on each of the organization's computing systems.

SW-13 Ensure the organization's application control system only allows the use of authorized software scripts on each of the organization's computing systems.

SW-14 Ensure the organization's application control system only allows the use of authorized operating system shells (such as Microsoft PowerShell or BASH) on each of its computing systems.

SW-15 Define a process the organization shall use to remove unauthorized software from each of its computing systems in a timely manner.

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.