Network Device Management Policy

(Last Updated April 2025)

Purpose

Our Network Device Management Policy aims to establish a comprehensive framework for the secure configuration, monitoring, and management of network devices within our organization. This policy aims to provide clear guidelines and procedures for properly administering, maintaining, and protecting network devices, including routers, switches, firewalls, and wireless access points. This policy seeks to minimize the risk of unauthorized access, data breaches, and network disruptions by implementing effective network device management practices. By enforcing secure configurations, regular patch management, and proactive monitoring, we strive to ensure our network infrastructure's availability, integrity, and confidentiality, protect against emerging threats, and maintain compliance with industry standards and regulatory requirements. By prioritizing network device management, we strengthen our overall cybersecurity posture, optimize network performance, and maintain the trust and confidence of our stakeholders.

Scope

The Network Device Management Policy applies to all our organization's employees, contractors, and stakeholders and encompasses the management and control of network devices within our IT infrastructure. This policy covers all network devices, including routers, switches, firewalls, wireless access points, and other networking equipment. It sets forth guidelines for device configuration, monitoring, and maintenance to ensure network communications' availability, integrity, and security. The policy defines procedures for device inventory, regular updates, patch management, and vulnerability scanning to mitigate risks associated with network devices. It also outlines the responsibilities of individuals involved in network device management processes, including network administrators, IT managers, and security personnel. 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 network device management and cybersecurity governance.

Safeguards

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

NDM-01 Maintain an inventory of each of the organization's approved network devices.

NDM-02	Maintain network device cybersecurity configuration benchmarks for the organization's authorized network devices.
NDM-03	Ensure the organization's network devices are managed from an approved, dedicated management network subnet.
NDM-04	Ensure the organization's network devices are not managed from a remote (or Internet-based) network.
NDM-05	Ensure the organization's network devices are managed from an approved Privileged Account Management (PAM) system or management jump box.
NDM-06	Ensure the organization's network devices require using Multi-Factor Authentication (MFA) to access the device.
NDM-07	Ensure the organization's network devices use encrypted remote management protocols (such as SSH or TLS).
NDM-08	Maintain a network device management system to manage each organization's approved network device.
NDM-09	Ensure the organization's network device management system regularly scans for new network devices to add to the organization's network device inventory.
NDM-10	Ensure the organization's network device management system monitors each network device's status and logs and alerts when it is offline.
NDM-11	Ensure the organization's network device management system performs IP Address Management (IPAM) for each network (including DHCP scopes).
NDM-12	Ensure the organization's network device management system records netflow data from each network device.
NDM-13	Ensure the organization's network device management system compares each network device's configuration on a regular basis to log and alert any changes to the configuration.
NDM-14	Ensure the organization's network device management system ensures that each network device utilizes the latest firmware for the network device.

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.