Cybersecurity Policy Templates

Vulnerability Management Policy

(Last Updated April 2025)

Purpose

Our Vulnerability Management Policy aims to establish a systematic and proactive approach for identifying, assessing, prioritizing, and remediating vulnerabilities within our organization's technology infrastructure. This policy aims to provide clear guidelines and procedures for monitoring, analyzing, and mitigating vulnerabilities to reduce the risk of exploitation and unauthorized access. By implementing effective vulnerability management practices, this policy seeks to enhance the security and resilience of our systems, protect sensitive information, and maintain compliance with industry standards and regulatory requirements. Through vulnerability scanning, penetration testing, and vulnerability remediation processes, we strive to identify and address security weaknesses in a timely manner, minimize potential threats, and safeguard the confidentiality, integrity, and availability of our data and networks. By prioritizing vulnerability management, we actively manage risk, improve our overall cybersecurity posture, and ensure the trust and confidence of our stakeholders.

Scope

The Vulnerability Management Policy applies to all our organization's employees, contractors, and stakeholders and encompasses the proactive identification, assessment, prioritization, mitigation, and monitoring of vulnerabilities within our IT infrastructure. This policy covers all systems, applications, network devices, and endpoints vulnerable to security flaws and weaknesses. It establishes guidelines for vulnerability scanning, penetration testing, risk assessment, and remediation processes. The policy sets forth procedures for vulnerability reporting, tracking, and patch management to ensure timely and effective resolution of identified vulnerabilities. It also defines the roles and responsibilities of individuals involved in vulnerability management processes. 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 vulnerability management and cybersecurity governance.

Safeguards

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

VUL-01	Maintain a Vulnerability Management (VM) system to detect and track weaknesses in the organization's information systems.
VUL-02	Ensure the organization's Vulnerability Management (VM) system uses agents and/or authenticated scans to detect weaknesses in the organization's information systems.
VUL-03	Ensure the organization's Vulnerability Management (VM) system scans for weaknesses caused by outdated, vulnerable software (based on CVEs).
VUL-04	Ensure the organization's Vulnerability Management (VM) system scans for weaknesses caused by software misconfigurations (based on CCEs).
VUL-05	Ensure the organization's Vulnerability Management (VM) system scans for open, dangerous network ports or services.
VUL-06	Ensure the organization's Vulnerability Management (VM) system prioritizes the vulnerabilities it detects in its information systems.
VUL-07	Ensure the organization's Vulnerability Management (VM) system compares the results of consecutive vulnerability scans to track the progress of remediation efforts over time.
VUL-08	Ensure the organization's Vulnerability Management (VM) system tracks open vulnerabilities in the organization's information systems.
VUL-09	Ensure the organization's Vulnerability Management (VM) system tracks approved exceptions when vulnerabilities are discovered on the organization's information systems.
VUL-10	Ensure the organization's Vulnerability Management (VM) system reports discovered vulnerabilities to the organization's technical staff regularly.

VUL-11 Ensure the organization's Vulnerability Management (VM) system regularly reports discovered vulnerabilities to the organization's business unit staff.

VUL-12 Ensure the organization's Vulnerability Management (VM) system reports discovered vulnerabilities to the organization's business leadership staff regularly.

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.