Cybersecurity Policy Templates

System Protection Management Policy

(Last Updated April 2025)

Purpose

Our System Protection Policy aims to establish a comprehensive framework for effectively managing and securing endpoints, including desktops, laptops, mobile devices, and other network-connected devices within our organization. This policy aims to provide clear guidelines and procedures for endpoint configuration, monitoring, patching, and access control to mitigate the risk of unauthorized access, data breaches, and malware infections. By implementing robust endpoint management practices, this policy seeks to enforce consistent security controls, protect against emerging threats, and ensure our data and systems' confidentiality, integrity, and availability. Through endpoint hardening, vulnerability management, and remote management capabilities, we strive to enhance our overall cybersecurity posture, minimize the attack surface, and maintain the trust and confidence of our stakeholders. By prioritizing endpoint management, we establish a strong defense against potential cyber threats, enable effective incident response, and support secure remote access and productivity.

Scope

The System Protection Policy applies to all our organization's employees, contractors, and stakeholders. It encompasses implementing and managing security measures to protect endpoints, including desktops, laptops, mobile devices, and servers, from cyber threats. This policy covers all endpoints connected to the organization's network, whether company-owned or personal devices used for work purposes. It sets forth guidelines for deploying and configuring endpoint protection solutions such as antivirus, antimalware, host intrusion prevention systems, and device encryption. The policy defines procedures for regular updates, monitoring, and enforcement of endpoint protection controls. 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 endpoint protection and cybersecurity governance.

Safeguards

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

SYS-01	Maintain an Endpoint Detection and Response (EDR) system to detect and alert malicious activity on the organization's computing systems, whether onsite or remote.
SYS-02	Ensure that the organization's Endpoint Detection and Response (EDR) system utilizes software agents that cannot be disabled by standard computing system users.
SYS-03	Ensure the organization's Endpoint Detection and Response (EDR) system is centrally managed and cloud-based.
SYS-04	Ensure that the organization's Endpoint Detection and Response (EDR) system's anti-malware signature is regularly updated on all computing systems.
SYS-05	Ensure the organization's Endpoint Detection and Response (EDR) system automatically scans removable media for potentially malicious files.
SYS-06	Ensure that the organization's Endpoint Detection and Response (EDR) system logs and tracks all running processes for cybersecurity incident response.
SYS-07	Ensure that the organization's Endpoint Detection and Response (EDR) system generates a database of the signatures (hashes) for all the files on each of the organization's computing systems for cybersecurity incident response.
SYS-08	Ensure that the organization's Endpoint Detection and Response (EDR) system logs and alerts on appropriate events for cybersecurity incident response.
SYS-09	Maintain host-based firewalls on each of the organization's computing systems.

SYS-10	Ensure the organization's host-based firewalls are configured with a default rule to deny all network traffic.
SYS-11	Maintain a whole-disk encryption system on the organization's endpoint computing systems.
SYS-12	Maintain a host-based Data Loss Prevention (DLP) system on each organization's computing system.
SYS-13	Maintain removable media safeguards on each of the organization's endpoint computing systems.
SYS-14	Ensure the organization's removable media safeguard system creates an inventory of authorized storage and peripheral devices.
SYS-15	Ensure the organization's removable media safeguard system tracks data owners on approved devices responsible for the media.
SYS-16	Ensure the organization's removable media safeguard system disables removable storage media on computing systems that do not require such devices.
SYS-17	Ensure the organization's removable media safeguard system disables unauthorized peripheral devices on computing systems that do not require such devices.
SYS-18	Ensure the organization's removable media safeguard system only allows reading and writing on authorized removable media devices.
SYS-19	Ensure the organization's removable media safeguard system only allows writing to authorized removable media devices utilizing encryption.

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.