Cybersecurity Policy Templates

Perimeter Network Access Management Policy

(Last Updated April 2025)

Purpose

Our Perimeter Network Access Policy aims to establish a comprehensive framework for effectively filtering and monitoring network traffic entering and exiting our organization's network boundaries. This policy aims to provide clear guidelines and procedures for implementing boundary filtering technologies, such as firewalls, intrusion prevention systems, and secure web gateways, to enforce network security controls, protect against unauthorized access, and mitigate the risk of external threats. By implementing robust boundary filtering practices, this policy seeks to minimize the risk of malicious activities, such as unauthorized access attempts, malware infections, and data exfiltration. By configuring appropriate filtering rules, continuous monitoring, and regular updates, we strive to ensure our network resources' confidentiality, integrity, and availability, safeguard sensitive information, and maintain compliance with industry standards and regulatory requirements. By prioritizing boundary filtering, we strengthen our overall cybersecurity posture, enhance network resilience, and maintain the trust and confidence of our stakeholders.

Scope

The Perimeter Network Access Policy applies to all our organization's employees, contractors, and stakeholders. It encompasses implementing and managing boundary filtering mechanisms to protect our network from unauthorized access and malicious activities. This policy covers all network boundaries, including external connections such as internet access points, virtual private networks (VPNs), and remote access services. It sets forth guidelines for configuring and maintaining boundary filtering technologies, such as firewalls, intrusion prevention systems (IPS), and network access control (NAC) solutions. The policy defines procedures for monitoring and filtering network traffic at the boundaries to enforce security policies, prevent unauthorized access, and detect and block malicious activities. 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 boundary filtering and cybersecurity governance.

Safeguards

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

PNA-01	Maintain an inventory of the organization's approved perimeter network connections (including Internet and third-party connections).
PNA-02	Maintain documented Access Control Lists (ACLs) for the organization's approved perimeter network connections.
PNA-03	Maintain perimeter network firewalls at the organization's approved perimeter network connections.
PNA-04	Ensure the organization's approved perimeter network firewalls perform IP-based filtering of perimeter network connections.
PNA-05	Ensure the organization's approved perimeter network firewalls perform protocol-based (TCP, UDP, or similar) inbound filtering of perimeter network connections.
PNA-06	Ensure the organization's approved perimeter network firewalls perform protocol-based (TCP, UDP, or similar) outbound filtering of perimeter network connections.
PNA-07	Ensure the organization's approved perimeter network firewalls perform application-based filtering of perimeter network connections.
PNA-08	Ensure that the organization's approved perimeter network firewalls perform user-based filtering of network connections, ensuring that only authorized users can remotely connect to an organization's network.
PNA-09	Ensure the organization's approved perimeter network firewalls require Multi-Factor Authentication (MFA) when authenticating all remote connections.
PNA-10	Ensure the organization's approved perimeter network firewalls use encrypted channels (such as TLS) when authenticating all remote connections.

PNA-11	Ensure the organization's approved perimeter network firewalls require User Behavior Analytics (UBA) when authenticating all remote connections.
PNA-12	Maintain a system to perform full packet capture for all of the organization's perimeter network traffic.
PNA-13	Maintain perimeter network Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) at the organization's approved perimeter network connections.
PNA-14	Maintain a perimeter web-based URL filtering system at the organization's Internet connections.
PNA-15	Ensure the organization's web-based URL filtering systems block network connections to unapproved web-based services (such as email, storage, or similar).
PNA-16	Ensure the organization's web-based URL filtering systems decrypt all TLS-encrypted traffic to facilitate web-based URL filtering.
PNA-17	Ensure that the organization's web-based URL filtering systems utilize Data Loss Prevention (DLP) on each of its Internet connections.
PNA-18	Ensure that the organization's perimeter network firewalls log appropriate events observed by the system.
PNA-19	Ensure that the organization's web-based URL filtering systems log all URLs observed by the system.
PNA-20	Ensure that the organization's Domain Name System (DNS) systems log all DNS queries observed by the system.
PNA-21	Ensure that the organization's Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) systems log all appropriate events observed by the system.
PNA-22	Ensure that the organization's perimeter network firewalls log all remote user connections observed by the system.

PNA-23 Maintain network deception technologies at the organization's perimeter network connections to facilitate incident detection and management.

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.