Cybersecurity Policy Templates

Internal Network Access Management Policy

(Last Updated April 2025)

Purpose

Our Internal Network Access Policy aims to improve security, performance, and control within our technology infrastructure. This policy guides the strategic implementation of network segmentation, aiming to limit the extent of potential cybersecurity threats, prevent unauthorized access, protect sensitive data, and ensure operational continuity. By segmenting our network and instituting robust controls, we aim to reduce the risk of internal and external attacks, minimize the impact of successful breaches, facilitate regulatory compliance, and uphold our commitments to stakeholders regarding safeguarding critical information assets.

Scope

The Internal Network Access Policy applies to all our organization's employees, contractors, and stakeholders and encompasses the implementation and management of network segmentation measures to enhance the security and resilience of our IT infrastructure. This policy divides our network into distinct segments or zones based on security requirements, business functions, and risk levels. It sets guidelines for configuring and enforcing network access controls, including firewalls, VLANs, and access lists, to restrict unauthorized access and contain potential threats. The policy defines procedures for network segmentation design, regular monitoring, and updates to ensure ongoing effectiveness. It also outlines the responsibilities of individuals involved in network segmentation 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 segmentation and cybersecurity governance.

Safeguards

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

INA-01	Maintain documented Virtual Local Area Networks (VLANs) for the organization's endpoint computing system networks.
INA-02	Maintain documented Virtual Local Area Networks (VLANs) for the organization's server computing system networks.
INA-03	Maintain documented Virtual Local Area Networks (VLANs) for the organization's hypervisor management system networks.
INA-04	Maintain documented Virtual Local Area Networks (VLANs) for the organization's software development networks.
INA-05	Maintain dedicated computing systems on dedicated Virtual Local Area Networks (VLANs) for high-risk computing activities.
INA-06	Maintain network authentication systems (802.1x) for each organization's wired network.
INA-07	Ensure that the organization's network authentication systems (802.1x) for each of its wired networks require certificate-based authentication.
INA-08	Maintain network authentication systems (802.1x) for each organization's wireless network.
INA-09	Ensure that the organization's network authentication systems (802.1x) for each of its wireless networks require certificate-based authentication.
INA-10	Ensure the organization's network authentication systems (802.1x) for each of the organization's wireless networks require the use of AES-CCMP to encrypt all wireless connections.
INA-11	Ensure the organization's network authentication systems (802.1x) for each of the organization's wireless networks require the use of a dedicated wireless network for all devices (guests) not managed by the organization.

INA-12 Ensure the organization's network authentication systems (802.1x) for each of the organization's wired or wireless networks require health checks of computing systems prior to allowing them access to the network.

INA-13 Ensure that each of the organization's endpoint computing systems' Virtual Local Area Networks (VLANs) enforces privatization to prevent computing systems from communicating with other systems on the same VLAN.

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.