Cybersecurity Policy Templates

Privileged Account Management Policy

(Last Updated April 2025)

Purpose

Our Privileged Account Management Policy aims to establish a comprehensive framework for the secure management and control of privileged accounts within our organization. This policy aims to provide clear guidelines and procedures for granting, monitoring, and revoking privileges associated with administrative or privileged accounts. This policy seeks to minimize the risk of unauthorized access, data breaches, and insider threats by implementing effective privileged account management practices. By implementing strong authentication mechanisms, segregation of duties, and regular privileged account reviews, we strive to ensure that privileged access is granted only to authorized individuals, protect the confidentiality and integrity of our systems and data, and maintain compliance with regulatory requirements. By prioritizing privileged account management, we strengthen our overall cybersecurity posture, mitigate the potential for security incidents, and maintain the trust and confidence of our stakeholders.

Scope

The Privileged Account Management Policy applies to all our organization's employees, contractors, and stakeholders. It encompasses managing and controlling privileged accounts, which have elevated access privileges within our IT infrastructure. This policy covers all accounts with administrative or superuser rights, including system administrators, network administrators, and other privileged roles. It sets guidelines for creating, monitoring, and protecting privileged accounts, including strong authentication mechanisms, secure password management, and regular access reviews. The policy defines privileged account provisioning, deprovisioning, and session monitoring procedures to mitigate the risks associated with privileged access. It also outlines the responsibilities of individuals involved in privileged account management processes, including privileged account 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 privileged account management and cybersecurity governance.

Safeguards

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

PAM-01	Maintain an inventory of all privileged accounts configured on endpoint computing systems.
PAM-02	Maintain an inventory of all privileged accounts configured on server computing systems.
PAM-03	Maintain an inventory of all privileged accounts configured on network devices.
PAM-04	Maintain an inventory of all privileged accounts configured on enterprise business applications.
PAM-05	Ensure all privileged accounts on endpoint computing systems are authorized and dedicated privileged accounts are required.
PAM-06	Ensure that all privileged accounts on server computing systems are authorized and require dedicated privileged accounts.
PAM-07	Ensure all privileged accounts on network devices are authorized and require dedicated privileged accounts.
PAM-08	Ensure that all privileged accounts on enterprise business applications are authorized and require dedicated privileged accounts.
PAM-09	Ensure that all default privileged accounts are not using their default system credentials to authenticate to the system.
PAM-10	Ensure that the organization does not allow shared privileged accounts for workforce members except in documented cases for emergency access or via a Privileged Account Management (PAM) system.
PAM-11	Maintain a Privileged Account Management (PAM) or Password Manager (PM) system for documenting service, shared accounts, or shared secrets between workforce members.

PAM-12	Maintain a Privileged Account Management (PAM) system to automatically rotate the credentials (using unique credentials) for each endpoint or server computing system.
PAM-13	Maintain a Privileged Account Management (PAM) system to automatically rotate the credentials (using unique credentials) for each network device.
PAM-14	Ensure the organization's Identity Providers (IDPs) require Multi-Factor Authentication (MFA) for all privileged accounts.
PAM-15	Ensure the organization's Identity Providers (IDPs) logs and alerts when changes are made to privileged group memberships.
PAM-16	Ensure the organization's Identity Providers (IDPs) log and alert account logon events (successful and failed) for all privileged accounts.

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.