Access Control Policy Template

Principles and controls for protecting CUI

Access controls ensure that only authorized users and processes gain access to systems and data. This template helps you establish an effective access control policy aligned with the NIST SP 800-171 Access Control family.

Policy Overview

- Purpose: define how the organization limits access to information systems and CUI.
- Scope: apply to all personnel, devices and systems that store, process or transmit CUI.
- Principle of Least Privilege: grant only the minimum access necessary to perform duties.
- Separation of Duties: assign roles to prevent single points of control over critical functions.
- Information Flow Restrictions: control who can transfer information between systems and networks.
- Account Management: identify account types (privileged, non-privileged, service accounts) and establish provisioning and de-provisioning processes.

Access Control Procedures

- Implement multifactor authentication for all accounts and systems accessing CUI.
- Use non-privileged accounts for routine activities and restrict privileged operations to approved administrators.
- Establish session locks and automatic termination after defined periods of inactivity.
- Limit the number of consecutive failed login attempts and enforce strong password policies.
- Monitor and control remote access through managed access points and secure tunnels.
- Encrypt remote sessions and wireless communications to protect confidentiality.
- Route traffic for remote privileged commands through controlled access points and authorize wireless access before connecting.

[7] CSF Tools Access Control family outlines requirements for limiting system access to authorized users, controlling information flow, enforcing least privilege, separating duties and protecting remote sessions with encryption.

Monitoring & Review

- Generate audit logs for account creation, modification and deletion.
- Review access logs and privileged activities regularly to identify suspicious behavior.
- Perform periodic access reviews to validate that users still require assigned privileges.
- Disable or remove inactive or unnecessary accounts promptly.
- Use automated tools to detect and prevent unauthorized privilege escalation.

Wireless & Remote Access Controls

- Require authorization before enabling wireless access to the network.
- Encrypt wireless connections using strong protocols and keys.
- Route remote access through secure gateways with monitoring and logging.
- Restrict remote execution of privileged commands and use secure administrative channels.

This template provides a foundation. Tailor it to your organization's specific systems, roles and regulatory requirements and integrate it with your identity and access management processes.