Access Management Policy

(Last Updated April 2025)

Purpose

Our Access Management Policy aims to establish a comprehensive framework for controlling and managing user access to our organization's systems, applications, and data resources. This policy aims to provide clear guidelines and procedures for granting, reviewing, and revoking access privileges, ensuring that users have the appropriate level of access based on their roles and responsibilities. This policy seeks to minimize the risk of unauthorized access, data breaches, and insider threats by implementing effective access management practices. By implementing strong authentication mechanisms, role-based access controls, and regular access reviews, we strive to ensure that only authorized individuals can access sensitive information, protect the confidentiality and integrity of our systems and data, and comply with regulatory requirements. By prioritizing access management, we strengthen our overall cybersecurity posture, safeguard against unauthorized access, and maintain the trust and confidence of our stakeholders.

Scope

The Access Management Policy applies to all our organization's employees, contractors, and stakeholders. It encompasses managing and controlling user access privileges to systems, applications, and data resources within our IT infrastructure. This policy covers all accounts and credentials to authenticate and authorize individuals' access. It sets forth guidelines for user provisioning, role-based access control, and segregation of duties to ensure appropriate access levels are granted based on job responsibilities and the principle of least privilege. The policy defines user account creation, modification, and termination procedures, as well as password management, session management, and access revocation. It also outlines the responsibilities of individuals involved in access management processes, including system administrators, IT managers, and access administrators. 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 access management and cybersecurity governance.

Safeguards

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

AM-01 Define a process for creating and documenting roles and responsibilities for each of the organization's workforce members.

AM-02 Ensure that the organization's documented roles and responsibilities for workforce members consider the principle of separation of duties when defining roles.

AM-03 Maintain documented Access Control Lists (ACLs) for each computing system and business application system.

AM-04 Ensure that the organization's documented Access Control Lists (ACLs) for computing systems and business applications are based on the organization's defined roles for workforce members.

AM-05 Maintain Access Control Lists (ACLs) on computing system objects based on approved documentation, roles, and the principle of least privilege.

AM-06 Maintain Access Control Lists (ACLs) on computing system functions based on approved documentation, roles, and the principle of least privilege.

AM-07 Maintain Access Control Lists (ACLs) on code repositories based on approved documentation, roles, and the principle of least privilege.

AM-08 Ensure that the organization's Access Control Lists (ACLs) enforce encryption of data at rest on each of the organization's computing systems.

AM-09 Ensure that the organization's Access Control Lists (ACLs) enforce data encryption in transit on each computing system.

AM-10 Define a process for reviewing the organization's documented Access Control Lists (ACLs) on a regular basis.

AM-11 Define a process for reviewing the organization's Access Control List (ACL) documentation on a regular basis.

AM-12	Define a process the organization shall use to regularly review the organization's group or role membership used by the organization's Access Control Lists (ACLs) regularly.
AM-13	Ensure the organization's information systems log and alert changes to group or role memberships or configured Access Control Lists (ACLs).
AM-14	Ensure the organization's information systems log and alert changes to group or role memberships or configured Access Control Lists (ACLs).

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.