Identity Management Policy

(Last Updated April 2025)

Purpose

Our Identity Management Policy aims to establish a comprehensive framework for effectively managing and controlling user identities, access privileges, and authentication mechanisms within our organization. This policy aims to provide clear guidelines and procedures for creating, maintaining, and terminating user accounts, as well as enforcing access controls and authentication standards. By implementing robust identity management practices, this policy seeks to minimize the risk of unauthorized access, data breaches, and insider threats. Through strong authentication mechanisms, role-based access controls, and regular access reviews, we strive to ensure that only authorized individuals have appropriate access privileges, protect the confidentiality and integrity of our systems and data, and maintain compliance with regulatory requirements. By prioritizing identity management, we strengthen our overall cybersecurity posture, minimize the potential for security incidents, and maintain the trust and confidence of our stakeholders.

Scope

The Identity Management Policy applies to all our organization's employees, contractors, and stakeholders. It encompasses managing and controlling user identities, access privileges, and authentication mechanisms within our IT infrastructure. This policy covers all accounts and credentials to access organizational systems, applications, and data resources. It sets forth guidelines for user provisioning, access controls, password management, and account lifecycle management to ensure information assets' integrity, confidentiality, and availability. The policy defines procedures for identity verification, role-based access control, single sign-on, and multi-factor authentication. It also outlines the responsibilities of individuals involved in identity management processes, including system administrators, IT managers, and identity 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 identity management and cybersecurity governance.

Safeguards

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

ID-01	Maintain a Human Resources (HR) program to manage the organization's workforce members formally.
ID-02	Maintain a Human Resources Information System (HRIS) to track the status of each organization's workforce member.
ID-03	Ensure that the organization's Human Resources (HR) program performs background screening for each workforce member.
ID-04	Ensure that the organization's Human Resources (HR) program requires workforce members to agree to the organization's terms and conditions of employment or similar appropriate contracts.
ID-05	Ensure that the organization's Human Resources (HR) program includes a process for workforce members to return physical assets after their work with the organization.
ID-06	Ensure that the organization's Human Resources (HR) program includes a process for workforce members to return information assets after their work with the organization.
ID-07	Ensure that the organization's Human Resources (HR) program includes a process for workforce members to return authentication credentials after their work with the organization.
ID-08	Maintain an inventory of each Identity Provider (IDP) the organization approves.
ID-09	Ensure that the organization minimizes the number of Identity Providers (IDPs) it uses and utilizes centralized Single Sign On (SSO) solutions whenever possible.
ID-10	Maintain an inventory of each user account authorized by the Identity Provider (IDP).

ID-11	Maintain a configuration benchmark for each of the organization's authorized Identity Providers (IDPs).
ID-12	Ensure that the configuration benchmarks for each of the organization's Identity Providers (IDPs) do not allow workforce members to share accounts.
ID-13	Ensure that the configuration benchmarks for each organization's Identity Providers (IDPs) do not allow concurrent account logins.
ID-14	Ensure that the configuration benchmarks for each organization's Identity Providers (IDPs) do not allow account names to be reused within a defined period of time.
ID-15	Define a process the organization shall use to regularly perform identity reviews of each of the organization's Identity Providers (IDPs) to ensure only authorized accounts exist in the system.
ID-16	Maintain an identity management system to provision accounts for workforce members once automatically added to the organization's Human Resources Information System (HRIS).
ID-17	Maintain an identity management system to automatically de-provision accounts for workforce members once they are tagged as inactive in the organization's Human Resources Information System (HRIS).
ID-18	Ensure that the configuration benchmarks for each of the organization's Identity Providers (IDPs) require strong passwords.
ID-19	Ensure that the configuration benchmarks for each of the organization's Identity Providers (IDPs) require account lockouts if a defined threshold of failed login attempts is exceeded.
ID-20	Ensure that the configuration benchmarks for each organization's Identity Providers (IDPs) require that passwords be stored encrypted and hashed using salts.
ID-21	Ensure that the configuration benchmarks for each of the organization's Identity Providers (IDPs) require passwords to be transmitted only when encrypted.

ID-22	Ensure that the configuration benchmarks for each of the organization's Identity Providers (IDPs) require a process for secure password provisioning by the organization's helpdesk.
ID-23	Ensure that the configuration benchmarks for each of the organization's Identity Providers (IDPs) require using Multi-Factor Authentication (MFA).
ID-24	Ensure that the configuration benchmarks for each of the organization's Identity Providers (IDPs) require that unused accounts are automatically disabled after a period of not being used and/or require the use of expiration dates on each account.
ID-25	Ensure that the configuration benchmarks for each of the organization's Identity Providers (IDPs) require logging logon events for standard accounts (whether successful or failed).
ID-26	Ensure that the configuration benchmarks for each of the organization's Identity Providers (IDPs) require logging access to deactivated accounts.
ID-27	Ensure that the configuration benchmarks for each of the organization's Identity Providers (IDPs) require logging User Behavior Analytics (UBA) events.

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.