Identity, Credential, and Access Management Policy

From the Office of Chief Information Officer, State of Minnesota

Version: 1.7
Effective Date: 1/1/2016
Revised: 12/31/2024
Approved: John Israel, State Chief Information Security Officer **Date:** 03/20/2025

Policy Statement

The purpose of this policy is to establish the authority of the Identity, Credential, and Access Management Program (ICAM Program) to define and implement the Standards and guidelines for the controls that govern the issuance, maintenance, auditability, and risk assessments of all digital identities, both human and non-human, with access to the Executive Branch network, systems, and data. Identity and access management controls and processes must be in place to ensure users, systems, applications, and networks have appropriate access to only what is necessary to perform required tasks and functions.

Employees must abide by the terms of this policy. Employees who violate this policy may be subject to discipline, up to and including discharge.

It is the responsibility of all credential holders to exercise due care to protect and safeguard the credentials assigned to them. Credential holders shall report potential lost, compromised, or stolen credentials immediately.

Standards and Guidelines will cover Executive Branch:

Identity types:

1. Workforce
2. Technological (non-human)
3. Privilege Access Management
4. Contractor and Vendor (3rd Party)
5. Citizen and Partner

Primary Management Components:

1. Identity Management

2. Credential Management
3. Access Management
4. Authentication
5. Authorization
6. Federation
7. Bring Your Own Identity

Reason for the Policy

Appropriate security measures must be taken to protect data and services entrusted to the State by the public. Proper implementation of account management, access rights, password requirements and multi-factor authentication reduces the likelihood of a compromise to the confidentiality, availability, and integrity of State data.

Roles & Responsibilities

- Employees, Vendors, and Contractors
  - Be aware of and follow relevant information security policies, standards, and procedures.
  - Ensure information security is incorporated into processes and procedures.
  - Ensure vendors and contractors are following required information security controls.
  - Contact information security staff or email GRC@state.mn.us with questions about the information security policies, standards, or procedures.
- Supervisors and Managers
  - Ensure employees and contractors are proficient in the information security policies, standards and procedures that are relevant to their role.
  - Hold employees accountable for following the information security policies, standards, and procedures.
- Information Technology Personnel
  - Apply appropriate controls to the design, operation and maintenance of systems, processes, and procedures in conformance with the information security policies, standards, and procedures.
- Information Security Personnel
  - Develop, maintain, and assess compliance with the information security policies, standards, and procedures.
  - Develop, maintain, and implement a comprehensive information security program.
  - Provide training on information security policies, standards, and procedures.
  - Assist agencies and personnel with understanding and implementing information security policies, standards, and procedures.
- Agency Data Practices Personnel
  - Assist agencies and personnel with questions on proper data use, collection, storage, destruction, and disclosure.

Applicability

This policy applies to all departments, agencies, offices, councils, boards, commissions, and other entities in the executive branch of Minnesota State Government.

Related Information

Identity and Access Management Standard

Privileged Account Management Standard

State Standards and Authoritative Source Cross Mapping

Glossary of Information Security Terms

History

Table 1. Version History

Version	Description	Date
1.0	Initial Release	7/8/2015
1.1	Added Compliance Enforcement Date	12/29/2015
1.2	Updated Compliance Enforcement Date and Template	12/20/2016
1.3	Updated Compliance Enforcement Date and Template	10/26/2017
1.4	Modified document title and minor edits	3/10/2020
1.5	Renamed document, rewritten policy statement and grammatical fixes	10/1/2022
1.6	Formatting fixes and reference new PAM standard	10/1/2023
1.7	Added enforcement language; updated version and revision date	12/2/2024

Contact

GRC@state.mn.us