Identity, Credential, and Access Management Standard

From the Office of the Chief Information Officer, State of Minnesota

Version: 1.8
Issued: 1/1/2016
Revised: 12/31/2024
Approved: John Israel, State of MN Chief Information Security Officer **Date:** 2/27/2026

Standard Statement

The State must establish, maintain, and control authentication and access for users, systems, applications and networks. Access controls protect State data by only granting access to systems and data that is necessary for an individual's job responsibilities.

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

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
1	Entitlements	All access to systems or data, other than one time submission of data and read only access to data with a data protection categorization of Low, must be controlled using identification and authentication mechanisms. This access control must: • The Identity and Access Management (IAM) team, in collaboration with system/data owners will establish and maintain a list of roles and their associated rights/entitlements. • Assign privileges to individuals based on the individual's job classification and function. • Restrict privileges to the least needed for the individual or service to perform their role. • Deny all access that is not explicitly granted. • Remove all system access not explicitly required. • User Access is to be reviewed every two years to verify that access is only granted via current role definitions.	Low Moderate High
2	Unique IDs	All users must be assigned a unique ID to access systems or data. IDs must not be reused until all previous access authorizations are removed from the system, including all file accesses for that identifier but not before a period of at least seven (7) years has expired	Low Moderate High
3	Device, Service and Application Accounts	Device, service, and application accounts must be assigned to an account owner and must not be used by individuals to access the system interactively. These accounts and their associated passwords must be managed by the enterprise privileged access management tool. This control applies to accounts with passwords.	Low Moderate High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
4	Access Approval	Requests to create or modify accounts and access privileges must be documented and approved by the requestor's supervisor/manager and the data/system owner before access can be granted. Each request for access must define access needs including: • Systems and data that each user needs to access for their job function. • Level of privilege required (for example, user, administrator, etc.) for accessing resources. See the Privileged Access Management Standard for privileged access approval.	Low Moderate High
5	Account Management	The addition, deletion, and modification of user IDs, MFA factors, and other identifier objects must be restricted to authorized account administrators. All accounts must have a documented supervisor/manager and maintained if user transfers positions.	Low Moderate High
6	Access Recertification	All accounts must be reviewed upon changes in user role and at least annually for user accounts (Requirement for privileged and service accounts has been withdrawn. See Privileged Access Management Standard.) • The review must validate and recertify that all access privileges are still needed and authorized. • The results of the review must be documented, and unnecessary access privileges must be communicated to account administrators for removal. • Review documentation must be maintained by the account administrator for at least 2 years and made available to the Enterprise Identity and Access Management team upon request.	Moderate High
7	Privileged access review	Withdrawn. See Privileged Access Management Standard.	Low Moderate High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
8	Inactive Accounts	Inactive user accounts must be disabled and have entitlements removed after no more than 60 days of inactivity. • Constituents • Partners • Employees • Contractors Inactive non-user accounts (including service, system, and device accounts) must be disabled after 60 days of inactivity. Disable all accounts that are only used annually when not in use. When Possible, disabled user accounts must be deleted within 1 year.	Moderate High
9	Revoke Entitlements	Accounts and privileges that are no longer required must be removed or disabled within: • 8 hours of notification or identification of voluntary changes in access needs. • 1 hour of notification or identification for users that have been involuntarily terminated or for accounts with credentials that may have been lost or compromised.	Low Moderate High
10	Emergency Accounts	Emergency accounts must be disabled within 24 hours of last use.	Low Moderate High
11	Privileged access	Withdrawn. See Privileged Access Management Standard.	Low Moderate High
12	Privileged access Use	Withdrawn. See Privileged Access Management Standard.	Low Moderate High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
13	Remote Administrative Access	Withdrawn. See Privileged Access Management Standard.	Low Moderate High
14	Segregation of Duties	Access privileges must allow for the appropriate segregation of duties by: • Segregating duties of individuals as necessary, to prevent malicious activity by a single individual. • Ensuring that audit functions are not performed by personnel responsible for administering access control. • Maintaining a limited group of administrators (i.e., system administrators, application administrators, security administrators) with access based upon the users' roles and responsibilities. Each administrator must have their own ID. • Ensuring that critical functions and system support functions are divided among separate individuals. • Ensuring that system testing functions and production functions are divided among separate roles. • Ensuring access authorizations does not violate any required separation of duties. • Ensuring that an independent entity, not the Business Owner, System Developer(s)/Maintainer(s), or System Administrator(s) responsible for the information system, conducts information security testing of the system. Documenting separation of duties of roles for each information system / application.	
15	Vendor Access	Accounts used by vendors to access, support, or maintain system components via remote access must be: • Enabled only during the time needed. Disabled when not in use. • Monitored when in use. • Accessed only via multi-factor. • Must use an account with privileged access to perform administrative functions	Low Moderate High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
16	Group Accounts	Group, shared or generic IDs, passwords or other authentication methods must be restricted as follows: • Generic user IDs must be disabled or removed. • Shared admin account requirement withdrawn. See Privileged Access Management Standard. Shared and generic user IDs must not be used to administer any system components. • Passwords and other credentials for group/role accounts must be managed in the enterprise privileged access management solution to ensure passwords are changed.	Low Moderate High
17	Authentication	All users must be authenticated on all systems by using at least one of the following methods: • Something you know, such as a password or passphrase. • Something you have, such as a token device or smart card. • Something you are, such as a fingerprint. All authenticators must have sufficient strength for their intended use.	Low Moderate High
18	User Validation	The user's identity must be properly validated before any transaction that has information security implications including modifying or communicating any authentication credential—for example, performing password or token resets, provisioning new tokens, or generating new keys. Before an administrator can create a credential and assign it to an individual, that person must provide proof of their claimed identity.	Low Moderate High
19	First Time Passwords	First-time use and reset passwords/phrases must be: • Set to a unique value for each user following password complexity requirements. • Changed immediately after the first use. • Not stored in the ticketing system.	Low Moderate High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
20	Password Encryption	All authentication credentials (such as passwords/phrases) must be cryptographically protected during transmission and storage.	Low Moderate High
21	Password Length	Passwords must be at least: • 14 characters long for user accounts • Privileged access length requirements withdrawn. See Privileged Access Management Standard.	Low Moderate High
22	Password Complexity	Passwords must contain at least: • 3 of the 4 character types below for user accounts and all mainframe accounts. Withdrawn. See Privileged Access Management Standard. Character Types: • Lower case letters • Upper case letters • Numbers • Special characters The use of dictionary names or single words must be prohibited. For systems required to meet ARC-AMPE requirements, require at least four (4) changed characters or be sufficiently different from previous passwords as determined by the information system (where technology allows) when new passwords are created.	Low Moderate High
23	Minimum Password Age	Passwords/passphrases, except those created by an administrator on behalf of the user (e.g., during password resets) and those managed by a privileged access management system, must be in place for at least 1 day.	Low Moderate High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
24	Maximum Password Age	Passwords/passphrases must be changed at least: • Every 30 days for mainframe accounts. • Every 90 days for user accounts. • Privileged access max age requirement withdrawn. See Privileged Access Management Standard.	Low Moderate High
25	Password History	New passwords/phrases must be different from at least the previous 24 passwords/phrases used by that account.	Low Moderate High
26	Mobile Device Authentication	Password/PIN Authentication to mobile devices must be configured as follows: • New passwords/PINs must be different from the previous 12. • Device must lock after 15 minutes of inactivity. • Device wipes all data after 10 invalid access attempts. • Password/PIN must be at least 4 characters long. • Password/PIN must be changed every 180 days.	Low Moderate High
27	Voicemail PIN	Access to voicemail boxes must be controlled through a PIN. This PIN must be configured as follows: • At least 6 characters long for user access. • At least 12 characters long for receiving data with a categorization of High. • Not the same as the mailbox number. • Not sequential. • No repeating characters.	Low Moderate High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
28	Non-Password Authentication	Where authentication mechanisms other than passwords are used (for example, physical or logical security tokens, smart cards, certificates, etc.), these mechanisms must be controlled as follows: • Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. • Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access. • A defined registration process must be established for issuing, maintaining, and retrieving hardware tokens. When issuing a token, the individual receiving the token must be authorized and verified in person by a designated official. Mechanisms and links used to register authentication items (e.g., to register RSA tokens) must expire within 24 hours.	Low Moderate High
29	PKI-Based Authentication	Where PKI-based authentication is used, the system must: • Validate certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information. • Enforce authorized access to the corresponding private key. • Implement a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.	Low Moderate High
30	Mask Password	All passwords must be masked (i.e., made unreadable) during authentication prevent unauthorized individuals from viewing the password.	Low Moderate High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
31	Account Lockout	User accounts must be locked out after no more than: • 3 consecutive invalid logon attempts by that user during a 120-minute period for systems with a data protection categorization of High. • 5 consecutive invalid logon attempts by that user during a 120-minute period for systems with data protection categorization of Moderate. • 10 consecutive invalid logon attempts by that user during a 120-minute period for systems with data protection categorization of Low. • For administrator account requirements see the Privileged Access Management Standard The account must remain locked for at least 30 minutes or until unlocked by an administrator.	Low Moderate High
32	Inactivity Timeout	Sessions must be automatically locked after 15 minutes of inactivity. All information previously visible on the screen must be replaced with a publicly viewable image during the session lock. The user must be required to re-authenticate to reactivate the session.	Low Moderate High
33	Session Termination	The information system automatically terminates a user session after fifteen (15) minutes of inactivity	High
34	Multiple Sessions	Systems must prevent multiple concurrent active sessions for individual user accounts. System and application accounts must be limited to the number of concurrent sessions needed for their purpose and as documented in the system security plan.	High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
35	System Use Notification	A warning banner must be displayed prior to granting access to all internal networks, applications, databases, operating systems, workstations, servers, and network devices. Users must explicitly acknowledge the warning banner before being allowed access to the system. The system warning banner must include the following information: • The user is accessing a restricted government information system. • System usage may be monitored, recorded and subject to audit. • Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties. • Use of the system indicates consent to monitoring and recording. For publicly accessible systems a warning banner must be displayed before allowing access. The warning banner must include: • Notification of any monitoring, recording, or auditing that may occur. • Description of the authorized uses of the system. For systems containing Federal Tax Information, the warning banner must reference the civil and criminal penalty sections of Title 26 Sections 7213, 7213A and 7431	High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization

36	Remote Access	All remote network access originating from outside the network by personnel (including users and administrators) and all third parties, (including vendor access for support or maintenance) must:
		• Be authorized.
		• Authenticate using multi-factor authentication.
		  ○ At least one of the factors must be provided by a device separate from the system gaining access.
		• Utilize encrypted connections.
		• Connect through a limited number of approved managed network access control points.
		• Validate all computers and devices that require any access to a network or system are securely configured and meet at least the following security requirements:
		  ○ up-to-date system patches,
		  ○ current anti-virus software, and
		  ○ functionality that provides the capability for automatic execution of code disabled.
			Low
			Moderate
			High

37	International Access	Access to Federal Tax Information or systems containing federal tax information must be prohibited from locations outside of the United States.	High
38	Authorized Distribution	Users must ensure State data is only distributed to authorized personnel by: • Only allowing authorized personnel to view content on their screen. • Only including necessary and relevant information in system output such as reports and printouts. • Only distributing system output to individuals authorized to view all content.	Moderate High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
39	Database Access	All access to any database containing data with a data protection categorization of High (including access by applications, administrators, and all other users) must be restricted as follows: • All user access to, user queries of and user actions on databases are through programmatic methods. Users must be prevented from accessing database data files at the logical data view, field, or field-value level. • For databases that fall under the scope of the Payment Card Industry Data Security Standard (PCI-DSS) only database administrators have the ability to directly access or query databases. • Restrict database management utilities to only authorized database administrators. • Implement table-level access control. • Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).	High
40	Device Identification and Authentication	The system must uniquely identify and authenticate laptops, desktops, and mobile devices before establishing a connection.	High
41	Test Accounts in Production Environment	Accounts created for testing in a production environment must be disabled within 24 hours after testing has been completed.	Low Moderate High
42	Password Exposure	If a password is exposed or suspected to have been exposed to anyone other than the account owner, the password must be changed immediately.	Low Moderate High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
43	Storing Passwords in Browsers	Passwords must not be saved within a browser.	Low Moderate High
44	Prohibited Authentication Methods	Social media logins not explicitly approved by MNIT are prohibited for use in accessing State systems, applications, and data.	Low Moderate High

Table 1. Identity and Access Management Controls

Reason for the Standard

To ensure data can only be accessed by authorized personnel, systems and processes, identity and access management controls must be in place to limit access based on need to know and according to job responsibilities.

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 standard 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 Policy

Privileged Access Management Standard

State Standards and Authoritative Source Cross Mapping

Glossary of Information Security Terms

History

Table 2. 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	12/22/2016
1.3	Updated Compliance Enforcement Date and Template	10/26/2017
1.4	Scheduled Document Refresh	3/10/2020

Version	Description	Date
1.5	Numerous updates from IAM team	11/1/2021
1.6	Removed controls that are now address in the Privileged Access Management Standard; multiple changes requested by IAM team	10/1/2023
1.7	Added enforcement language; fixed references to PAM standard; changed minimum password length; added prohibited authentication methods control	12/2/2024
1.8	Replaced outdated MARS-E reference with ARC-AMPE	1/12/2026

Contact

GRC@state.mn.us