State of Nevada

Information Security Committee

Standard

Document ID	Title	Revision	Effective Date	Page
S.5.01.01	User Identification and Authentication	F	05/08/2025	1 of 6

1.0 PURPOSE

This standard establishes the minimum user identification and authorization requirements for Information Technology (IT) systems.

2.0 SCOPE

This standard applies to all state agencies and authorized users meeting the criteria identified in the State Information Security Program Policy, Section 1.2, Scope and Applicability.

3.0 EFFECTIVE DATES

This standard becomes effective at the time of approval of the State Chief Information Officer (CIO).

4.0 RESPONSIBILITIES

The agency head and appointed Information Security Officer (ISO) are responsible for ensuring the implementation of and compliance with this standard.

5.0 RELATED DOCUMENTS

State Information Security Program Policy, 100
Data Sensitivity, S.3.02.01
Access Controls and Audit Trails, S.5.02.02
Account Monitoring and Control, S.6.16.01

6.0 STANDARD

6.1 Secure Authentication Methods

A. Secure authentication to State resources requires either strong passwords or a multi-factor authentication solution.

B. Technology assets must support authentication requirements for the identified data classification level. Data will not be accessed, stored, transported or otherwise maintained on a device that is not in compliance with the identified data classification level.

C. Multi-factor authentication is the preferred method for providing secure authentication to state resources and, when used, must include at least two of the three authentication factors. Multi-factor authentication is highly encouraged for access to any systems containing confidential data.

D. Non-existent (blank) or default-supplied credentials are explicitly prohibited and must be changed before connection to any State IT resource.

E. Passwords must not be set to infinite expiration periods.

F. Passwords shall not be transmitted in “clear text” or make use of any protocol which uses “clear text”, unless the mode of transmission is encrypted.

6.2 User Identification

A. Each system user ID must uniquely identify only one user, whenever possible. Shared or group user authentication credentials (user IDs and passwords) are prohibited, unless the system only allows or recognizes a single user ID

6.3 Strong Passwords Minimum Construction

A. All passwords for State IT systems will adhere to the following minimum requirements, unless the hardware/software system is incapable of meeting these requirements:

   A. Passwords for standard user accounts must be a minimum of eight (8) characters long when always used with MFA, or 14 characters long without MFA. If a system does not support the minimum number of characters, then the maximum number of characters that the system supports must be used and compensating control(s) should be used, such as limiting IP addresses that can connect to the system.

      1. Passwords must not contain commonly-used, expected, or compromised values. Passwords must be validated against a dictionary of bad passwords, which includes:

         a. Passwords obtained from previous breaches
         b. Dictionary words
         c. Repetitive or sequential characters (e.g., ‘aaaaaaaa’, ‘1234abcd’)
         d. Context-specific words, such as the name of the service, the user’s first or last name, the username, and derivatives thereof.

B. When a newly selected password does not meet these requirements, users must be informed why the password was rejected and given an opportunity to select a different one.

C. The use of passphrases is encouraged. A passphrase is a series of words or other text that holds meaning to the user but not to others. When combined with the rules for complex passwords, passphrases can be very secure (e.g., MyBLu3NiS$@n, 0uRD0gM@x).

6.4 Administrator and Service Accounts

Dedicated administrator accounts must be used for administrative access on enterprise assets and must not be used to conduct general computing activities, such as internet browsing, email, and productivity suite use. Passwords for access to critical systems, administrative or elevated privileges, and service accounts must meet additional requirements for enhanced security protections, in addition to the minimum requirements for strong passwords:

A. MFA is required for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider. Where MFA is not

supported, access via an alternative method that supports MFA, such as a jump box, is strongly encouraged.

B. Passwords for access to critical systems must be separate and unique from any other system passwords, except for accredited multi-factor authentication or single sign-on solutions.
C. Passwords for service accounts and accounts with administrative or elevated privileges must be separate and unique from other system passwords.
D. Service accounts must not be used as administrator accounts.

Each service account shall be limited to logging onto the specific systems where it is designated to be used.

6.5 Acceptable Password Use

A. Each user must agree in writing:

1. Not to disclose or loan their credentials or multi-factor authentication access hardware.
2. To avoid using their state password or similar variations of it on non-state systems, such as websites. The use of agency-approved password management software is encouraged, especially for creating and maintaining unique passwords for each web site.
3. To change any password immediately if it has been disclosed (or suspected of being disclosed) to another party.
4. To report the loss of multi-factor authentication (MFA) access hardware to the Help Desk or their agency ISO immediately.

B. Users should have the option to display the password when entering it, rather than seeing a series of dots or asterisks. The password may be fully displayed using this option, or the individual characters may display for a short time after each character is typed.

C. The display and printing of passwords, PINS, and account user validation secrets must be masked, suppressed, or otherwise obscured to prevent unauthorized observation or recovery.

D. Maintaining a stored list of User ID and password combinations is prohibited, except in rare operational cases. Such lists must be stored in a secure location.

E. Passwords granting access to sensitive data or elevated system access must not be saved, stored, or hard-coded in plain-text format. Password hashes and passwords stored in encrypted files are permissible. Password hashing algorithms on State systems must be approved by the governing agency.

6.6 Account Password Changes

A. All account passwords must be changed at least every 365 days, but not more than once per day, as well as anytime a compromise or problem is suspected or reported.

The once per day requirement does not preclude the service desk from resetting a password for a positively identified user who reports a problem.

B. System managers must immediately change every potentially affected password on a system if password file integrity is, or is suspected of being, compromised. An incident response form must be completed and submitted to the Office of Information Security (OIS) after the passwords are changed.
C. Passwords cannot be re-used or rotated within ten previous password changes.

6.7 Account Lock Outs

A. All accounts shall be locked out after five consecutive unsuccessful logon attempts. The system may release a locked-out account after 15 minutes. If a system administrator assists with releasing a locked-out account and is reasonably certain of no unauthorized access, the 15-minute elapsed time is not applicable. If supported, the system should permanently lock the account and require IT involvement to unlock it.
B. If accounts are automatically released after 15 minutes, the agency will monitor all systems for repeated failed logon attempts that could indicate malicious activity.

6.8 Password Creation and Resets

Passwords cannot be entered or changed unless the system representative has taken reasonable steps to positively identify the requestor. All requests must be confirmed by:

A. Direct contact or voice recognition between the representative and the employee.
B. Confirmation from the employee's management or network administrator.
C. Correct responses for predefined keywords or phrases for manual or automated password changes.
D. Call-back initiated by the granting agency through the employee's immediate supervisor.

Temporary passwords must meet all other password requirements and require an immediate change to a permanent password.

7.0 DEFINITIONS

Credentials: A set of claims used to prove the identity of a client, containing an identifier and proof of identity, such as a password.

Multi-factor authentication: Two or more factors positively identifying a user, including:

1. Something you know (a password, PIN, mother's maiden name, etc.)
2. Something you have (a hardware token, smart card, smartphone, etc.)
3. Something you are (fingerprint, retina/iris scan, facial recognition, etc.)

Service accounts: Accounts used by automated system functions (services) that do not correspond to an actual person. These accounts are often built-in and used for automated

functions. However, some automated functions may require actual user accounts to perform certain functions, and may be employed using domain accounts to run services.

System Administrator: The individual responsible for maintaining the IT environment, including managing user accounts, modifying security parameters, and handling system logs and permissions.

- Add, change, or delete user accounts and associated user provisioning for database, operating system, and network layers;
- Modify operating system, database, and application security and policy parameters;
- Add, change, or delete system exception logging information; or
- Add, change, or delete permissions to data files and folders.

8.0 RESOURCES

Center for Internet Security (CIS), CIS Controls v8.0 Guide
CIS_Benchmarks_Password_Policy_Guide_v21.12

9.0 EXCEPTIONS

Requests for exceptions to this Information Security Standard must be documented, submitted to the Office of Information Security (OIS), and approved by the State Chief Information Security Officer (CISO).

Approved By

Title	Signature	Approval Date
State Information Security Committee	Approved by Committee	11/19/2020
State Chief Information Security Officer (CISO)	Signature on File	05/01/2025
State Chief Information Officer (CIO)	Signature on File	05/08/2025

State of Nevada

Information Security Committee

Standard

Document History

Revision	Effective Date	Change
A	2/21/2012	Replaces Standard 4.61 which was effective 5/9/02
B	5/21/2012	OIS Biennial review, replaces standard 4.150100
C	4/30/2017	Biennial review by SISC
D	12/26/2018	Renumbering (118 to S.5.01.01) and compliance to ADA standards
E	12/31/2020	Biennial review for alignment with CIS Controls v7.1, Implementation Group 1 (IG1)
F	08.14/24	Review for alignment with CIS Controls v8.0 and CIS_Benchmarks_Password_Policy_Guide_v21.12