



State of Nevada

Information Security Committee

Standard

| Control No. | Rev. | Title | Effective Date | Page |
|-------------|------|---|----------------|--------|
| 118 | B | User Identification and Authentication (Passwords) | 05/21/2012 | 1 of 3 |

1.0 PURPOSE

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

2.0 SCOPE

This standard applies to all state entity employees, contractors, and all other authorized users, including outsourced third parties, who have access to, use, store, transmit or manage state data or information within or for the Executive Branch of Nevada State Government.

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) have the responsibility to ensure the implementation of and compliance with this standard.

5.0 RELATED DOCUMENTS

State Information Security Consolidated Policy, 100, Section 5.1

6.0 STANDARD

Access to State systems must be adequately protected against unauthorized modification, disclosure or destruction. Secure authentication to State resources requires the following:

A. All passwords for State IT systems will adhere to the following minimum requirements:

- 1) Passwords must be a minimum of eight (8) characters long.
- 2) Passwords must include a combination of upper and lower case letters.
- 3) Passwords must include **at least** one number. (0-9)
- 4) Passwords must include **at least** one special character. (Ex: #, %, *, !, \$, etc.)
- 5) Users must not use any dictionary word (in any language) as a password.

B. Each user will agree in writing to not disclose their credentials to any other person and to change any password immediately if it has been disclosed (or suspected to have been disclosed) to another party.



State of Nevada

Information Security Committee

Standard

| Control No. | Rev. | Title | Effective Date | Page |
|-------------|------|---|----------------|--------|
| 118 | B | User Identification and Authentication (Passwords) | 05/21/2012 | 2 of 3 |

- C. Each system user-ID must uniquely identify only one user. Shared or group user-IDs and / or passwords are prohibited.
- D. The display and printing of passwords must be masked, suppressed or otherwise obscured so that unauthorized parties will not be able to observe or recover them.
- E. All passwords must be changed at least every 90 days, but not more than once per day unless a compromise is suspected or reported. Passwords must not be set to infinite expiration periods.
- F. Non-existent (blank) or default-supplied credentials are explicitly prohibited, and must be changed before connection to any State IT resource.
- G. Passwords granting access to sensitive data or elevated access to the system must not be saved, stored or hard-coded in any system or application.
- H. 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.
- I. Passwords cannot be re-used or rotated on a given system within three previous password changes.
- J. Any account shall be disabled on the third unsuccessful logon attempt until positively verified and re-enabled by an administrator.
- K. Passwords cannot be entered or changed in a computer system for authentication and authorization purposes unless the representative for the system granting access has taken reasonable steps to positively identify the requestor. All requests for entry or change of passwords must be confirmed by:
 - 1) Direct contact or voice recognition is established between the representative and employee.
 - 2) Confirmation is received from the employee's management or network administrator.
 - 3) The requestor has correct responses of predefined keywords / phrases for password changes.
 - 4) Call-back is initiated by the granting agency through the employee's immediate supervisor.
- L. Passwords for access to critical systems will be separate and unique from any other system passwords, with the exception of accredited multi-factor authentication or single sign-on solutions.
- M. Multi-factor authentication is recommended for access to any systems containing confidential data.



State of Nevada

Information Security Committee

Standard

| Control No. | Rev. | Title | Effective Date | Page |
|-------------|------|---|----------------|--------|
| 118 | B | User Identification and Authentication (Passwords) | 05/21/2012 | 3 of 3 |

7.0 DEFINITIONS

Credentials: A set of claims used to prove the identity of a client. They contain an identifier for the client and a proof of the client's identity, such as a password. They may also include information, such as a signature, to indicate that the issuer certifies the claims in the credential.

Multi-factor authentication: Two or more factors positively identifying a user. Examples of multi-factor authentication include, but are not limited to biometric readers and authentication tokens.

8.0 EXCEPTIONS/OTHER ISSUES

Requests for exception to the requirements of this Information Security Standard must be documented, provided to the office of Information Security (OIS), and approved by the State Chief Information Security Officer (CISO).

| <i>Approved By</i> | | |
|--|-----------------------|------------|
| Title | Signature | Date |
| State Information Security Committee | Approved by Committee | 10/27/2011 |
| State Chief Information Security Officer (CISO) | Signature on File | 2/21/2012 |
| State Chief Information Officer (CIO) | Signature on File | 5/21/2012 |

| <i>Document History</i> | | |
|-------------------------|---------|--|
| Revision | Date | Change |
| A | 2/21/12 | Replaces Standard 4.61 which was effective 5/9/02 |
| B | 5/21/12 | Office of Information Security biennial review, replaces standard 4.150100 |
| | | |