State of Nevada

Information Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
118	C	User Identification and Authentication (Passwords)	08/29/2017	1 of 5

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-issued system-IDs used by state entity employees, contractors, and all other authorized users, including outsourced third parties and members of the general populace, to access, use, store, transmit, or manage state data or information residing on any state-owned or leased equipment 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
State Data Sensitivity Standard,111

6.0 STANDARD

Access to State systems must be adequately protected against unauthorized modification, disclosure, or destruction. Secure authentication to State resources requires either strong passwords or a multi-factor authentication solution to include the following:

A. 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.

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

1) Passwords for standard user accounts must be a minimum of eight (8) characters long. Passwords for administrative accounts, or accounts with elevated privileges, must be a minimum of twelve (12) characters long.

2) Passwords must not contain values known to be commonly-used, expected, or compromised. Passwords must be validated against a dictionary of bad passwords before being allowed on any state system. The dictionary should include, but is not limited to:

   i. Passwords obtained from previous breaches.

   ii. Dictionary words

   iii. Repetitive or sequential characters (e.g. ‘aaaaaaaa’, ‘1234abcd’).

   iv. Context specific words, such as the name of the service, the user’s first or last name, the username, and derivatives thereof.

3) When a newly selected password does not meet these requirements, the users must be told to select a different password, why the password was rejected, and given an opportunity to select a different value.

C. 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.

D. The use of passphrases should be encouraged. A passphrase is a series of words or other text strung together that hold meaning to the user but not to anyone else. When combined with the rules for complex passwords they can be very secure (Ex: MyBLu3NiS$@n, 0uRD0gM@x).

E. Each user will agree in writing to not disclose or loan their credentials or access hardware to any other person, to change any password immediately if it has been disclosed (or suspected to have been disclosed) to another party, and to immediately report the loss of their access hardware to the Help Desk or their agency ISO when it is identified as missing.

F. Each system user-ID must uniquely identify only one user, whenever possible. Shared or group user-IDs and / or passwords are likewise prohibited, unless the hardware/software system only allows/recognizes a single user-ID.

G. The display and printing of passwords/PINS/secrets must be masked, suppressed or otherwise obscured so that unauthorized parties will not be able to observe or recover them.

H. All user passwords must be changed at least every 90 days, but not more than once per day, as well as anytime a compromise or problem is suspected or reported.

I. Service account passwords are an exception to this rule and must be changed at least annually. Passwords must not be set to infinite expiration periods.

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

K. 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 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 and must use a 32-bit or longer salt value. LANMAN hashes of passwords are strictly prohibited.

L. 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.

M. Passwords cannot be re-used or rotated on a given system within ten previous password changes.

N. All accounts shall be locked out on the third-consecutive unsuccessful logon attempt. The system may release a locked-out account after 30 minutes has elapsed. If a system administrator assists with releasing a locked-out account, and is reasonably certain of no unauthorized user access, the elapsed time of 30 minutes is not applicable.

    1) If locked-out accounts are automatically released after 30 minutes, the agency will monitor all systems for repeated failed logon attempts which could indicate malicious activity.

O. The use of agency approved password management software is allowed and should be encouraged.

P. 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 for predefined keywords / phrases for manual or automated password changes.

    4) Call-back is initiated by the granting agency through the employee's immediate supervisor.

Q. 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.

R. Passwords for accounts with administrative or elevated privileges must be separate and unique from other system passwords.

S. 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.

T. User IDs that are inactive on the system for 30 days or more should be disabled.

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. The factors that make up multi-factor authentication include:

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 on which automated system functions (services) are dependent to execute. A service account does not correspond to an actual person. These are often built-in accounts that an automated system function (service) uses to access resources it needs in order to perform its activities. 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(s) responsible for maintaining the stable operation of the IT environment (including software and hardware infrastructure and application software) and/or has system authorization/access to perform the following administrative function(s):

- 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 EXCEPTIONS/OTHER ISSUES

State of Nevada

Information Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
118	C	User Identification and Authentication (Passwords)	08/29/2017	5 of 5

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).

Approved By		
Title	**Signature**	**Date**
State Information Security Committee	Approved by Committee	7/20/2017
State Chief Information Security Officer (CISO)	Signature on File	8/17/2017
State Chief Information Officer (CIO)	Signature on File	8/29/2017

Document History		
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
C	4/30/17	Biennial review by SISC