



State of Nevada

Information Technology Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
4.61	A	Password	05/09/02	1 of 3

1.0 PURPOSE

This standard establishes the minimum Password Standards for Information Technology (IT) systems.

Information handled by processing systems and associated data communications networks must be adequately protected against unauthorized modification, disclosure or destruction. Effective passwords minimize opportunities for computer crime. Properly constructed passwords improve the likelihood that users are who they claim to be and that a user's access can be controlled effectively. Good passwords are an important deterrent to intrusion and an effective means of identifying an individual and preventing access to information, provided the secrecy of the password is maintained.

2.0 SCOPE

This standard applies to all state agencies meeting the requirements identified in the State IT Security Policy, Section 2.0 Scope.

3.0 EFFECTIVE DATES

The requirements of this standard are effective 90 days after sign-off by the Governor or his designee.

4.0 RESPONSIBILITIES

The agency head or appointed Information Security Officer (ISO) has the responsibility to ensure implementation and compliance with this standard.

5.0 RELATED DOCUMENTS

State IT Security Policy 4.02
State Information Security Officer (ISO) Roles and Responsibility, 4.03

6.0 STANDARD

6.0.1 PASSWORD CONTROLS

User-IDs are used to establish the identity of an individual and establish accountability for access to controlled information. A password is an electronic key assigned to a specific person that authenticates their identity. The standards for the establishment and control of user-ID's and passwords are as follows.

- A) The ability to execute business transactions on behalf of the State shall be restricted by both individual user identification and positive authentication (password) of the person using that ID.
- B) Each computer and communication system user-ID must uniquely identify only one user. Shared or group user-IDs and passwords are prohibited. Any exception to this standard (e.g. training) requires the specific need to be properly documented and approved by the agency ISO.



State of Nevada

Information Technology Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
4.61	A	Password	05/09/02	2 of 3

- C) Each user shall agree in writing to not disclose a password to any other person and to change the password promptly if it has been disclosed to anyone else. Exceptions are only allowed with approval from the ISO or system administrator.
- D) Vendor-supplied default passwords must be changed before any computer or communications system is used for State business.
- E) System managers must immediately change every password on a system if password file integrity is, or is suspected of being compromised.
- F) 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.
- G) All user passwords shall be changed at least every 90 days.
- H) To prevent password guessing attacks, the number of consecutive attempts to enter an incorrect password shall be strictly limited. After three (3) unsuccessful attempts to enter a password, the involved user-ID shall be disabled until verified and reset or re-enabled by systems administration.
- I) 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 password(s) must be confirmed by either:
 - 1) Direct contact or voice recognition between the representative and employee.
 - 2) Confirmation from the employee's management or network administrator.
 - 3) Knowledge of predefined keywords or phrases by the requestor for password changes.
 - 4) Call-back initiated by the granting agency through the employee's immediate supervisor.

6.0.2 PASSWORD CONSTRUCTION

System environments permitting, passwords shall:

- A) Be a minimum of eight characters long.
- B) Include uppercase and lowercase letters, special characters and numbers.

7.0 DEFINITIONS

None



State of Nevada

Information Technology Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
4.61	A	Password	05/09/02	3 of 3

8.0 EXCEPTIONS/OTHER ISSUES

Request for exception to the requirements of this IT Security Standard must be documented, provided to and approved by the State IT Security Committee and Chief Information Officer (CIO).

<i>Approved By</i>		
Title	Signature	Date
State IT Security Committee Chair	Signature on File	08/29/2001
NV IT Operations Committee Chair	Signature on File	05/09/2002
Governor/Governor's Representative	Signature on File	06/17/2003

<i>Document History</i>		
Revision	Date	Change
A	05/09/02	Initial release.