State of Nevada
Information Security Committee

Standard

Document ID	Title	Revision	Effective Date	Page
S.5.02.02	Access Controls and Auditing	E	9/03/2019	1 of 3

1.0 PURPOSE

This standard establishes the minimum Access Control and Auditing Standards 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 Program Policy 100, Section 5.2 Data Access Controls
State Information Security Program Policy 100, Section 5.3 Audit Trails

6.0 STANDARD

Information handled by processing systems and associated data communications networks shall be adequately protected against unauthorized modification, disclosure or destruction. Effective controls for access to information resources minimize inadvertent employee error and negligence and reduce opportunities for computer crime. Properly implemented and managed access controls will improve the likelihood that users are who they claim to be and that a user's access can be controlled effectively. Access controls are an important deterrent to intrusion.

6.1 User Access Controls

The following access control standards will apply:

A. All data shall be protected by access controls, comparable to the level of classification, to ensure that it is not improperly disclosed, modified, deleted or rendered unavailable.

B. All agreements or contracts with individuals or groups, other than state employees, must identify the access requirements as part of the contract.

C. System Managers shall reevaluate system access privileges granted to all users quarterly.

D. Access rights and privileges for every State system shall be reviewed in the event of a change of access, whether by termination of contract, termination of employment, revocation of rights, reassignment, or other separation from agency, department, or service.

E. Agencies that retain or have been given stewardship of data are responsible for determining who may have access to the data. Criteria shall be established in granting each user or class of user access to information/data. The criteria shall be based on the concept of least privilege. Least privilege is based on the user's job function, the minimum set of privileges required to perform that function, and the need to have separation of duties. The separation of duties shall be based on the sensitivity of the system or information accessed to prevent an individual from having all necessary authority or information access to allow fraudulent activity without collusion.

F. System managers must be able to produce a report of user IDs and access rights for their system upon demand, for the support of investigations and audits.

G. Maintaining a stored list of User-ID and password combinations is prohibited. The sole exception would be those rare occasions where a list of this type is an operational requirement. In this case, agencies shall store the list in a secure storage location.

H. Access to data considered sensitive or private, or mandated to be so, shall be controlled using digital identity devices, encryption software or evolving secure identity methods. It is the responsibility of the agency to research, classify, and protect the data accordingly prior to allowing access to the data.

I. All systems must present a warning banner approved by the agency, that meets all governance requirements applicable to that agency.

6.2 Auditing

A. Agencies shall assess appropriate logging levels for systems they are responsible for and document logging procedures for security purposes. Logging procedures will be reviewed at least annually.

B. All agencies must maintain a change control process for documenting system administrative changes or updates to production systems.

C. All system and application logs shall be maintained in a form that cannot readily be viewed or altered by unauthorized persons.

D. Agencies must regularly analyze logs to identify unauthorized activity.

E. Audit trail information will be retained for an appropriate amount of time based on requirements applicable to the agency.

F. Any software required to read or generate reports from log files must be retained at least as long as the log files.

7.0 DEFINITIONS

None

8.0 RESOURCES

N/A

State of Nevada

Information Security Committee

Standard

9.0 EXCEPTIONS

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	Approval Date
State Information Security Committee	Approved by Committee	7/25/2019
State Chief Information Security Officer (CISO)	Signature on File	8/01/2019
State Chief Information Officer (CIO)	Signature on File	9/03/2019

Document History

Revision	Effective Date	Change
A	5/09/2002	Initial release
B	9/12/2002	Revision of Section 6.2
C	5/31/2012	Renumbering and minor revisions, replaces standard 4.60
D	12/26/2019	Renumbering (114 to S.5.02.02) and compliance to ADA standards.
E	7/25/2019	Review and updates for access and logging standards