State of Nevada

Information Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
114	C	Access Controls and Auditing	6/4/2012	1 of 4

1.0 PURPOSE

This standard establishes the minimum Access Control and Auditing Standards for Information Technology (IT) systems.

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.

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 5.2 and 5.3

6.0 STANDARD

6.0.1 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. Public access data will be tightly controlled using the best practices of the technology industry to ensure the authenticity of the transaction, to include the identity of the user in order to input, modify, or delete data created by them.

D. A person shall not attempt to access without authorization, State and department computer systems or networks outside the scope of work required.

E. System Managers shall reevaluate system access privileges granted to all users annually, at a minimum.

F. A System/User Master List of all users and their respective user-ID codes shall be maintained, kept secured and up-to date, reflecting all computer systems each person has access to so that their privileges may be expediently revoked on short notice. Access rights and privileges for every State system shall be included to ensure quick notification is given to all system administrators of those systems 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.

G. 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 privileged which 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.

H. System Managers are responsible for managing and maintaining a list of user access rights and user-Ids for each system to which they have access.

I. The ISO shall review the System/User Master List to verify accuracy and document the results on an annually basis.

J. 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 facility.

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

6.0.2 AUDITING

Mainframes, servers, or Local Area Networks (LAN) computer systems shall securely log all significant computer security relevant events. Examples of these events include: password guessing attempts; unauthorized transactions; attempts to use privileges that have not been authorized; modification to production application software; and modification to system software.

A. Agencies shall conduct an assessment of 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. Dataflow diagrams must be available for auditing purposes.

C. All agencies must maintain a change control process for documenting system administrative changes or updates to production systems. Any items that are determined to fall outside that realm must be agreed upon in writing by agency ISO's and management staff.

D. All system and application logs shall be maintained in a form that cannot readily be viewed or altered by unauthorized persons. A person is unauthorized if he or she is not a member of the internal audit staff, agency security staff, system management staff, or if he or she does not need to have such access to perform regular duties.

E. Security personnel will review each computer's log information at an appropriate time interval based on the sensitivity of the system's data.

F. Audit trail information will be retained for an appropriate amount of time based on requirements defined by the agency.

G. 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 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).

State of Nevada

Information Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
114	C	Access Controls and Auditing	6/4/2012	4 of 4

Approved By		
Title	**Signature**	**Date**
State Information Security Committee	Approved by Committee	5/31/2012
State Chief Information Security Officer (CISO)	Signature on File	6/4/2012
State Chief Information Officer (CIO)	Signature on File	6/4/2012

Document History		
Revision	**Date**	**Change**
A	05/09/02	Initial release.
B	09/12/02	Revision of Section 6.0.2
C	5/31/12	Renumbering and minor revisions, replaces standard 4.60