State of Nevada

Information Security Committee

Standard

Document ID	Title	Revision	Effective Date	Page
S.3.04.01	Personnel Security	J	9/13/2024	1 of 4

1.0 PURPOSE

This standard establishes the minimum personnel security requirements for users of State information and information technology (IT).

2.0 SCOPE

This standard applies to all state agencies and authorized users meeting the criteria identified in the State Information Security Program Policy, Section 1.2, Scope and Applicability.

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 agency Information Security Officer (ISO) have the responsibility to ensure the implementation of and compliance with this standard.

Agency management and personnel staff are responsible for coordinating and cooperating with the ISO to ensure compliance with the requirements of this standard.

5.0 RELATED DOCUMENTS

NAC 284.317 Investigations of applicants; minimum age requirement.
State Information Security Program Policy, 100
Information Security Officer (ISO) Roles and Responsibilities, S.3.03.01

6.0 STANDARD

6.1 Sensitive Positions

A. Positions shall be identified and classified with regard to the sensitivity of the data they control or process, and the facilities to which they have access. Agency managers and ISOs shall use the following guidelines to determine sensitive positions, if the position:

1. Has a major responsibility for the development, planning, direction, or implementation of a computer system.
2. Has a major responsibility for the development, planning, direction, or implementation of a computer security program.
3. Has approval authority for major component of a computer system, including hardware and software.
4. Has the ability to cause grave damage to a system or realize significant personal gain through their access or responsibility.
5. Has the potential for detrimentally impacting computer security.
6. Has duties of considerable importance to the agency IT mission, with significant program responsibilities.

7. Has access to, or affect the processing of, proprietary data or privileged information.

B. The following IT positions, roles and duties, at a minimum, shall be identified as sensitive:

1. Managers
2. Security/Compliance Officers
3. Systems Administrators
4. Systems Maintenance
5. Network Administrators
6. Database Administrators
7. Programmers
8. Backup Administrators
9. NCAS Partition Administrators
10. IT Generalists
11. Contractors and Vendors who work for or provide IT services to the state.

C. Employees temporarily assigned to duties that are deemed sensitive in nature are in sensitive positions for the duration of that assignment and must comply with the requirements of this standard.

D. Employees who will hold sensitive positions shall have pre-employment screenings, which are documented and maintained within the agency Personnel File. Please refer to NAC 284.317 as a guideline for such screenings.

E. All agencies will comply with existing state and federal laws, and regulations that impose significant responsibilities on employees for the security of information.

F. Employees shall sign a Letter of Agreement and/or Non-disclosure Agreement before access is allowed to information or information systems indicating that they understand their role and responsibilities for securing information and protecting information technology. These requirements shall normally be accomplished through the New Employee Orientation and/or Information Security Awareness Training.

G. Sensitive positions shall have critical functions divided among different individuals (separation of duties), whenever possible, to ensure that no individual has all necessary authority or information access that could result in fraudulent activities and misuse of confidential/privileged information.

6.2 Background Checks

A. Fingerprint-based background checks shall be conducted on all persons hired, promoted, changed duties, have enhanced responsibilities, or contracted for all positions determined to be sensitive. This requirement is supported by NRS 239B, Disclosure of Personal Information to Governmental Agencies.

B. The agency may absorb the applicable fees for fingerprinting and background checks. Fingerprinting must be done by a law enforcement agency.

C. Unfavorable results from a background check are not an automatic cause to refuse employment or cause termination. The agency head, after consulting with the agency personnel office, has the final decision on action to be taken or not taken based on any

unfavorable results. The agency head, after consulting with the agency personnel office, shall consider a conviction in any jurisdiction of any crime involving moral turpitude or indicating a lack of business integrity or honesty, whether denominated a felony or misdemeanor, to be an unfavorable result of a background check.

D. A list of agency employees/contractors holding sensitive positions as provided in Section 6.0 shall be maintained by the agency ISO. The list shall be updated within 30 days of any change in status (e.g. new hire appointment completion date, termination, functional responsibility change, etc.). The list shall include: name of employee/contractor; functional IT responsibility; status of background investigation; and date of completed appointment.

6.3 Termination

A. Agencies will establish, implement, and maintain procedures for processing terminations, both voluntary and involuntary, of employees. The procedures for processing termination involving sensitive positions or access to sensitive information shall be more restrictive than those in non-sensitive positions.

B. When an employee is involuntarily terminated from employment, all system access privileges will be immediately revoked and the employee is to be prevented from having any opportunity to access information or equipment.

6.4 Tracking and Reporting

A. Agency ISOs will be responsible for ensuring a list of employees in sensitive positions within their agency is maintained. The list will include, at a minimum, the position title, PCN, name of the incumbent, and date the last background check for that individual was performed. The list will be reviewed and reported to the agency head on a regular basis, quarterly at a minimum.

7.0 DEFINITIONS

State Agency: The use of the term “State agency” in this standard means every agency, bureau, board, commission, department, division, or any other unit of the Executive Branch of the government of the State of Nevada.

8.0 RESOURCES

N/A

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).

State of Nevada

Information Security Committee

Standard

Approved By

Title	Signature	Approval Date
State Information Security Committee	Approved by Committee	8/29/2024
State Chief Information Security Officer (CISO)	Signature on file	9/13/2024
State Chief Information Officer (CIO)	Signature on file	9/13/2024

Document History

Revision	Effective Date	Change
A	2/14/2002	Initial release
B	12/12/2002	Revisions to incorporate background checks
C	12/11/2003	Revision to section 6.0.1 paragraph B, sensitive position information
D	10/03/2006	Review by ITSPC, changed 6.0 paragraph C.1 reference to NRS to NAC
E	6/30/2011	Revision to update background check requirements, section 6.1
F	1/22/2015	Office of Information Security biennial review, replaces standard 4.04
G	9/29/2016	Changes to Section 6.1 (A) and (D)
H	12/26/2018	Renumbering (105 to S.3.04.01) and compliance to ADA standards
I	12/31/2020	Biennial review for alignment with CIS Controls v7.1, Implementation Group 1 (IG1). Changes for consistency with State Information Security Program Policy vE.
J	9/13/2024	Changes to 6.1(B), addition of 6.1(C) and 6.4