# State of Nevada

***Information Security Committee***

# Standard

| Document ID | Title | Revision | Effective Date | Page |
|---|---|---|---|---|
| S.3.03.01 | Information Security Officer (ISO) Roles and Responsibilities | E | 12/31/2020 | 1 of 4 |

## 1.0 PURPOSE

This standard identifies the responsibilities of the agency appointed Information Security Officer (ISO).

## 2.0 SCOPE

This standard applies to all state agencies 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

Agency heads have the responsibility to ensure that their agency complies with the requirements of this Security Standard.

## 5.0 RELATED DOCUMENTS

State Information Security Program Policy, 100

## 6.0 STANDARD

### 6.1 Agencies

Agencies shall appoint, in writing, one or more ISOs dependent on the organizational structure, who shall be responsible for development, implementation, management, training, and enforcement of policies and standards regarding the security of information and information technologies, which includes all divisions, bureaus, boards, and commissions under the agency's purview, regardless of physical office location.

### 6.2 Selection Standards

A. The appointed ISO shall have sufficient authority to enforce the information security policy and standards.

B. The appointed ISO shall have as a minimum sufficient high-level classification such that the duties of the position may be effectively executed.

C. The appointee must understand:

1. The need for collecting, storing, archiving, and using sensitive information.

2. The need for information privacy.

3. The rights and desires for personal and corporate privacy.

4. The availability of State and Federal laws and policies, standards, and procedures regarding information security, confidentiality, and privacy.

5. The techniques, devices and methods of Physical Security (restricting access to machines, rooms and buildings).

6. The techniques, devices and methods of Access Security (restricting access to information elements via machines).

D. The appointment of the ISO shall be announced to all agency staff and the State Information Security Committee Chair, located in Enterprise IT Services (EITS) within 15 working days of the formal appointment.

**6.3 ISO Responsibilities**

A. Act as principle advisor to their organization on information security issues.

B. Be a member of the State Information Security Committee and serve as the primary point of contact for the State Information Security Committee Chair.

C. Develop, implement, and maintain an information assets risk management and assessment program.

D. Develop, implement, maintain, and enforce an Information Security Plan consistent with the State Information Security Policy and Standards to ensure the proper protection of information technologies and information against unauthorized or accidental modification, destruction or disclosure.

E. Establish procedures to monitor and conduct internal reviews to evaluate compliance with the established agency Information Security Plan to include, but not limited to, review of software inventories for license compliance, risk analyses, and the adequacy of implemented safeguards.

F. Report, at least annually to the agency head, the status and effectiveness of the Information Security Plan.

G. Serve as the internal and external point of contact on Information Security matters.

H. Participate in the appointment of staff with specific information security responsibilities in divisions, bureaus, boards, and commissions, including remote offices. Assist the appointees in understanding and accomplishing Information Security responsibilities.

I. Provide input on security safeguards in the development or acquisition of new IT systems.

J. Oversee procedures for password control and user access to IT systems.

K. Ensure schedules and procedures for adequate system and data backup and recovery are in place.

L. Oversee or be a member of a team in developing, maintaining, and testing IT Contingency, Disaster Recovery and Business Resumption Plans.

M. Coordinate, report, and document any suspected or actual breach of security or computer crime with the appropriate management and State Information Security Committee Chair.

N. Ensure that a current list of critical applications is maintained.

O. Ensure that valid asset inventory information is available, current, and auditable, including inventories of hardware, software, applications systems, and system users.

P. Coordinate an Information Security Awareness Training Program that ensures all users are informed of Information Security policies, standards, and procedures.

Q. Review the new employee orientation process to ensure knowledge and understanding of information security policies, standards, and procedures are addressed.

**7.0 DEFINITIONS**

None

**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).

**Approved By**

| Title | Signature | Approval Date |
|---|---|---|
| State Information Security Committee | Approved by Committee | 11/19/2020 |
| State Chief Information Security Officer (CISO) | Signature on File | 11/24/2020 |
| State Chief Information Officer (CIO) | Signature on File | 11/30/2020 |

# State of Nevada

***Information Security Committee***

## Standard

| Document ID | Title | Revision | Effective Date | Page |
|---|---|---|---|---|
| S.3.03.01 | Information Security Officer (ISO) Roles and Responsibilities | E | 12/31/2020 | 4 of 4 |

**Document History**

| Revision | Effective Date | Change |
|---|---|---|
| A | 2/14/2002 | Initial release |
| B | 1/22/2015 | Office of Information Security biennial review, replaces standard 4.03 |
| C | 8/28/2016 | State Information Security Committee biennial review with no changes |
| D | 12/26/2018 | Renumbering (102 to S.3.03.01) and compliance to ADA standards |
| E | 12/31/2020 | Biennial review for alignment with CIS Controls v7.1, Implementation Group 1 (IG1) |