# State of Nevada
***Information Security Committee***

# Standard

| Document ID | Title | Revision | Effective Date | Page |
|---|---|---|---|---|
| S.4.08.02 | Information Security Incident Management | E | 10/26/2022 | 1 of 4 |

## 1.0 PURPOSE

This standard establishes minimum requirements to ensure all information security incidents will be reported and responded to systematically, taking appropriate steps to minimize loss or theft of information, or disruption of services.

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

## 5.0 RELATED DOCUMENTS

NRS 205.473 to 205.513, Unlawful Acts Regarding Computers and Information Systems
NRS 242.181, Adherence by using agencies and elected officers of State to regulations; reporting of certain incidents;
NRS 281.195, Use of Computers
State Information Security Program Policy, 100
Information Security Incident Report Form, S.4.08.02.1F

## 6.0 STANDARD

### 6.1 Information Security Incident Reporting

Any and all security incidents that may have, or have, affected, degraded, or violated either production systems; or Federal, State, or agency security policy, standards, or procedures shall be documented.

A. All information security incidents shall be documented by completing an Information Security Incident Report Form (S.4.08.02.1F) containing at a minimum:

1. Description of incident
2. Date and time
3. Impact on the agency and/or IT resource
4. Estimated financial impact
5. Mitigation action taken
6. Preventative Action Recommendations
7. Name, title and date of the person completing the report

B. All documented Information Security Incident Reports shall be provided to the Office of Information Security (OIS) within three (3) working days. If the incident is critical, as determined by the unit manager or designee, immediate notification of OIS must occur.

C. OIS shall review and maintain all Information Security Incident Reports and follow through with required actions or recommendations. Follow through actions must also be documented and attached to the original Information Security Incident Report.

D. OIS and/or the affected agency shall notify the Division of Risk Management immediately, but no later than 10 days after discovery of any incidents that meet any of the following criteria:

   a. Any incidents where notifications to individuals or third parties are required.

   b. Any incidents where PII or other sensitive information has been exposed.

   c. Any incidents requiring forensic investigation.

   d. Any incidents where the cost of response or notification may have the potential of exceeding the current insurance deductible of $250,000.

E. OIS shall provide statistics on incidents to the Chief Information Officer (CIO), Chief Information Security Officer (CISO), and State Information Security Committee at minimum quarterly.

### 6.2 Information Security Incident Response

A. When a security incident occurs, the initial incident response must follow these minimum response steps. There are two types of information security incidents, characterized incidents and uncharacterized incidents.

   1. When a **characterized** security incident occurs, the functional unit responsible for the affected systems will follow the unit's existing desk procedures to correct or mitigate the impact. If the incident or related outage exceeds two hours of production (six hours non-production system) downtime, the functional unit will create a report describing the root cause of the issue and the steps taken to resolve the incident, with submission to OIS who will track incidents and consolidate into the CIO and CISO report.

   2. When an **uncharacterized** security incident occurs, the functional unit will inform OIS after two hours of production (six hours non-production system) downtime and work to mitigate, isolate, identify the issue, and otherwise protect the forensic integrity of the situation while working to resolve the incident. During this time the functional unit will take every care to preserve all available data for analysis and future investigation. Once the incident has been characterized the functional unit will submit a report to OIS.

B. If an incident remains uncharacterized for six hours the functional unit will submit a status report to OIS.

### 6.3 Cyber Security Incident Response Team

At any time during an information security incident, characterized or uncharacterized, the CIO or CISO may create a Cyber Security Incident Response Team (CSIRT).

A. The CISO shall coordinate the establishment of an incident response team, if necessary; identify the individuals who will participate in the incident response; and consult with the agency on whether technical resources available to the agency have the expertise required for the type of incident, or if external incident response resources are needed.

B. The function of this team is to ensure a systematic response to an incident, minimizing loss of information, minimizing disruption of services, and maximizing preservation of data, log files, and configuration information pertinent to the incident.

C. Post-incident actions include ensuring functional units update their desk procedures, configurations, and documentation as required to minimize future impacts of the same incident. The CSIRT Lead will follow-up with a finalized report to the CIO and CISO.

## 7.0 DEFINITIONS

**Characterized Incident**: An incident or event that is precisely defined and understood. Characterized incidents may have occurred previously. Documentation of characterized incidents should include corrective actions.

**Uncharacterized Incident**: An incident or event that is not understood. Un-characterized incidents have not occurred previously.

**Information Security Incident**: Any abnormal occurrence that negatively impacts the operation of state IT systems or information, or the ability of users to utilize state IT resources; and may include a loss of data confidentiality; disruption of data or system integrity; disruption or denial of availability; or a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

**Physical Security Incident**: An occurrence which impacts or jeopardizes the controls in place to protect the physical structure or environment of a building, office, vehicle, and all resources within; such as secure doors being propped open, vandalism, theft, suspicious vehicles located near the department's sensitive buildings, inappropriate location of IT equipment (i.e., lack of environmental or physical protection for the device), etc.

**Administrative Security Incident**: An occurrence to where administrative security controls are violated such as badges not being worn, sign in/out logs not completed, etc.

**Desk Procedure**: A set of documented steps to perform a specific function. An example is the set of actions required to update virus signature files on a desktop.

## 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 | 09/27/2022 |
| State Chief Information Security Officer (CISO) | Signature on File | 10/24/22 |
| State Chief Information Officer (CIO) | Signature on File | 10/26/22 |

**Document History**

| Revision | Effective Date | Change |
|---|---|---|
| A | 11/2/2011 | Initial release |
| B | 1/22/2015 | OIS biennial review, replaces standard 4.140800 |
| C | 12/26/2018 | Renumbering (108 to S.4.08.02) and compliance to ADA standards |
| D | 12/31/2020 | Biennial review for alignment with the CIS Controls v7.1, Implementation Group 1 (IG1) |
| E | 09/27/2022 | Added notification to Division of Risk Management |