



State of Nevada

Information Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
4.140800	A	Security Incident Management	11/02/11	1 of 4

1.0 PURPOSE

This standard establishes a process that ensure all IT, physical and administrative 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 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) and/or the Chair, State IT Security Committee.

4.0 RESPONSIBILITIES

The agency head and appointed Information Security Officer (ISO) has the responsibility to ensure the implementation of and compliance with this standard.

5.0 RELATED DOCUMENTS

State Information Security Program Policy 4.100000, Section 4.8
Security Incident Management Flow diagram, 4.140800D
Security Incident Management Report Form, 4.140800F

6.0 STANDARD

6.0.1 Security Incident Reporting

Any and all security incidences that may or have affected, degraded or violated either production systems or departmental or state security policy, standards or procedures shall be documented.

A. All security incidents shall be documented by completing a Security Incident Report Form (4.140800F) containing at a minimum:

- 1) Description of incident
- 2) Date and time
- 3) Impact on the agency and/or IT resource



State of Nevada

Information Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
4.140800	A	Security Incident Management	11/02/11	2 of 4

- 4) Estimated financial impact
- 5) Mitigation action taken
- 6) Preventative Action Recommendations
- 7) Name, title and date of the person completing the report

- A. All documented 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.
- B. OIS shall review and maintain all Security Incident Reports and follow through with required actions or recommendations. Follow through actions must be documented also and attached to the original Security Incident Report.
- C. OIS shall provide statistics on incidents to the Chief Information Officer (CIO), Chief Information Security Officer (CISO), and State Security Committee at minimum quarterly.

6.0.2 Security Incident Response

- A. This procedure establishes the process that is followed when an IT incident occurs. There are two types of incident, characterized incidents and uncharacterized incidents.
 - 1) When a **characterized** IT 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 with submission to OIS who will track incidents and consolidate into the CIO and CISO Report.
 - 2) When an **uncharacterized** IT 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.
- C. At any time during an IT incident, characterized or uncharacterized, the CIO or CISO may create a Computer Incident Response Team (CIRT).



State of Nevada

Information Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
4.140800	A	Security Incident Management	11/02/11	3 of 4

- D. The administrative lead of this team will be the Department of Administration ISO or the CIO/CISO's designee.
- E. The function of this team is to ensure a systematic response to an incident, minimizing loss of information, minimizing disruption of services and preservation of data, log files and configuration information pertinent to the incident.
- F. Post-incident actions include ensuring functional units update their desk procedures, configurations and documentation as required to minimize future impacts of the same incident as well as the CIRT 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.

IT Security Incident: Any abnormal occurrence that negatively impacts the operation of state IT systems or information and/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, a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Physical Security Incident – is 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 - is 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 EXCEPTIONS/OTHER ISSUES

Guidance for Exceptions is provided in State Information Security Policy, 4.100000, appendix A.



State of Nevada

Information Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
4.140800	A	Security Incident Management	11/02/11	4 of 4

<i>Approved By</i>		
Title	Signature	Date
State IT Security Committee	Approved by Committee	10/27/11
State Committee Chair/State CISO	Signature on File	11/02/11
State Chief Information Officer	Signature on File	11/02/11

<i>Document History</i>		
Revision	Date	Change
A	11/02/11	Initial release.