State of Nevada

Information Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
107	C	Administrative Investigations of IT Security Incidents and Breaches	11/17/2016	1 of 2

1.0 PURPOSE

The purpose of this standard is to establish the criteria and requirements for the Office of Information Security (OIS) to conduct administrative investigations of computer technologies including but not limited to inappropriate or unauthorized system or application use, access, or manipulation of system integrity or data.

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 Chief Information Officer (CIO), Chief Information Security Officer (CISO) and the affected agency head have the responsibility to ensure the implementation and compliance with this standard.

5.0 RELATED DOCUMENTS

NRS 281.195, Use of Computers
State Information Security Consolidated Policy, 100, Section 3.1.1

6.0 STANDARD

6.0.1 INVESTIGATION REQUEST AND AUTHORIZATION

A. Requests for investigation of situations that involve information resources or alleged to violate published federal, state or departmental regulation or policy involving technical resources must be presented in written form by the requesting agency's appointing authority to the CIO on agency letterhead.

B. The Chief Information Officer (CIO) must approve investigation requests.

C. OIS shall assume the lead for all EITS coordination efforts, conducting the investigation and reporting of all requested investigations.

6.0.2 INVESTIGATION

A. The CISO shall coordinate the establishment of an investigation team, if necessary, identify the names of the individuals who will partake in the investigation, and identify who will be authorized to:

1) Access the computer

2) Examine the information stored or retrieved from the computer

3) Archive, maintain, store, transfer, transmit or destroy information retrieved from the computer

B. The CISO may develop Office of Information Security (OIS) Standard Operating Procedures (SOPs) outlining additional OIS procedures.

C. The OIS shall maintain a record of all investigations using a Confidential Investigation Log Form.

D. All documents/working papers involved with an investigation are confidential, whereby, requiring that all documents related to the investigation be controlled as such by OIS.

7.0 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).

Approved By		
Title	**Signature**	**Date**
State Information Security Committee	Approved by Committee	11/17/2016
State Chief Information Security Officer (CISO)	Signature on File	11/18/16
State Chief Information Security Officer (CIO)	Signature on File	11/18/16

Document History		
Revision	**Date**	**Change**
A	2/21/12	Initial release.
B	1/22/15	Office of Information Security biennial review, replaces standard 4.130100
C	11/17/16	Reviewed by State Information Security Committee with no changes