State of Nevada

Information Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
111	D	Data Sensitivity	01/22/2015	1 of 2

1.0 PURPOSE

This standard establishes the minimum Information Technology (IT) Data Sensitivity standards.

All IT systems must include security controls that reflect the true importance of the information processed on the system and the agency's investment embodied in the components of the IT system. To accomplish this the sensitivity of the data is measured by the need to protect data from loss, destruction, misuse, unauthorized disclosure/access, modification, unavailability or any other security vulnerability.

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 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

State Information Security Consolidated Policy, 100, Section 3.2.3

6.0 STANDARD

6.0.1 Sensitivity of Information

A. All agencies shall determine the sensitivity of information in accordance with state and federal policies, regulations and laws.

B. Sensitivity classification shall include, but not limited to the following criteria:
   1) The information that requires protection from unauthorized disclosure.
   2) The information, which must be protected from unauthorized or unintentional modification.

6.0.2 Protection of Information

A. All agencies shall determine, develop and implement a plan of protection based on the classification and degree of sensitivity of the information.
B. Protection of sensitive information will include the following:
   1) Sensitive information in existing legacy applications will encrypt data as is practical.
   2) Confidential Personal Data will be encrypted whenever possible.
   3) Sensitive Data will be encrypted in all newly developed applications.

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	10/27/2011
State Chief Information Security Officer (CISO)	Signature on File	2/21/2012
State Chief Information Officer (CIO)	Signature on File	1/22/2015

Document History		
Revision	**Date**	**Change**
A	08/08/02	Initial release.
B	2/21/12	Renumbering – minor revisions
C	4/25/12	Office of Information Security biennial review, replaces standard 4.130200
D	01/22/2015	Added encryption language to Sections 6.0.1 and 6.0.2