State of Nevada

Information Security Committee

Standard

Document ID	Title	Revision	Effective Date	Page
S.3.02.01	Data Sensitivity	G	12/31/2020	1 of 2

1.0 PURPOSE

This standard establishes the minimum Information Technology (IT) Data Sensitivity requirements. All IT systems must include security controls that reflect the true importance of the information processed on the system, the need to protect the data in the IT system, and the agency's investment embodied in the components of the IT system.

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

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 Security Program Policy, 100

6.0 STANDARD

6.1 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 is 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.

6.2 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 DEFINITIONS

Sensitive Data: Information or data that requires security controls reflecting the true importance of the information, based on the agency's investment in and dependence on the information. Security controls are required to protect the information from loss, destruction, misuse, unauthorized disclosure/access, modification, unavailability or any other security vulnerability. Examples include but are not limited to information or data:

- containing Personal Information as defined by NRS 603A.040,
- regarding the security of information systems as declared Confidential per NRS 242.105, or
- declared as classified, sensitive, or protected by other state or federal laws or regulations.

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

Document History

Revision	Effective Date	Change
A	8/08/2002	Initial release
B	2/21/2012	Renumbering – minor revisions
C	4/25/2012	OIS biennial review, replaces standard 4.130200
D	1/22/2015	Added encryption language to Sections 6.0.1 and 6.0.2
E	12/26/2018	Renumbering (111 to S.3.02.01) and compliance to ADA standards
F	2/27/2020	Added explicit definition for "Sensitive Data"
G	12/31/2020	Biennial review for alignment with CIS Controls v7.1, Implementation Group 1 (IG1)