State of Nevada

Information Security Committee

Standard

Document ID	Title	Revision	Effective Date	Page
S.4.03.01	Electronic Media Security	C	12/31/2020	1 of 4

1.0 PURPOSE

This standard establishes the minimum requirements for the protection of state data, the marking of the portable or mobile media containing the data, as well as the sanitization and disposal of the electronic media that stored the data.

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

State Information Security Program Policy, 100

6.0 STANDARD

6.1 Media Protection

A. Electronic media must be protected from pilferage, misuse, or unauthorized access to ensure and preserve the confidentiality, integrity, and availability of the data.

B. All electronic media must be protected based on the value of the media and data it contains versus the cost of the protection, without regard to who purchased or owns the media or data.

C. Electronic media put in storage must be provided double barrier protection, e.g., locked office within a locked building; a locked, theft resistant container, with a locked office; or a locked building within a locked fenced area.

D. Electronic media, including portable/mobile media, containing confidential, restricted, or sensitive data not in the presence of the authorized user must be secured within a locked environment.

E. Confidential data residing on portable/mobile media must be protected through encryption and password protection.

6.2 Media Marking

A. All types of electronic media, e.g., removable electronic media, disk drives, CDs, DVDs, external hard drives and portable devices, mobile devices, USBs and serials must be labeled to indicate the identity of the data steward and sensitivity level of the data.

B. Labeling will include the agency name, employee name, the data sensitivity and date created, e.g., EITS, Jane Doe, Confidential PERS, MM/DD/ YYYY.

C. Electronic media that has been used, or is believed not to be blank, must be labeled. New, unused media requires no labeling until it is used.

D. Media containing multiple files with varying sensitivity requires the media to be labeled indicating the highest level of sensitivity and protected at that level.

6.3 Sanitization and Disposal

A. All technology assets will undergo electronic media sanitization before being transferred, donated, or otherwise disposed of by appropriate agency IT personnel. This sanitization will overwrite all information on electronic media with a minimum of three (3) passes with random information overwritten on each pass. Technology assets that contain confidential or personal identification information (PII) during their service life must utilize a minimum of seven (7) passes with random information overwritten on each pass.

B. Sanitization or disposal of leased electronic media equipment (e.g., computer hard drives, copy machines) MUST ensure that residual data may not be easily retrieved and reconstructed as outlined in DOD Memorandum, 8 January 2001 for the Destruction of DoD Computer Hard Drives Prior to Disposal.

C. Current leased equipment requires a special risk assessment prior to the end of the lease/disposal.

D. The value of the data must be weighed against the replacement cost of the media.

1. Media costing less than the value of the data will be destroyed, making the data unrecoverable. National Institute of Standards and technology (NIST) Special Publication (SP) 800-88 will be used for guidance.

2. Media costing more than the value of the data will be sanitized. Sanitization is the process of removing data from storage media, with reasonable assurance that in proportion to the sensitivity of the data, the data may not be retrieved and/or reconstructed.

E. The sanitization of electronic media that has contained “sensitive material” will be recorded and maintained in a log for historical reference which contains the following information:

1. Date/time of disposition/sanitization/transfer
2. Business function from which the media derived
3. Data steward who was responsible for the media
4. Type of media being sanitized/transferred
5. Sensitivity level of the data on the media

F. The disposition log will have columns that will allow for the annotation of disposition/transfer or destruction of the media.

G. The disposition log will have columns that will allow for the annotation of inventory data, time, location and individual performing the inventory.

H. Documentation of media disposition will be recorded and retained in a log for historic reference.

I. A certificate of media disposition is required for all media that has ever contained “sensitive material”.

J. A certificate of media disposition is required for all media that is released from state service.

K. A certificate of media disposition is required for all media that is transferred from one state agency to another.

L. The media disposition log and certificates will be reconciled with the physical inventory of equipment whenever a new entry is made in the log.

7.0 DEFINITIONS

Technology Assets: As defined in CIS Controls v7.1, the term “Technology Assets” (also referred to therein as “Hardware Technology Assets” or “Hardware Assets”) collectively refers to equipment and devices that have the potential to store or process information, whether connected to the network or not.

8.0 RESOURCES

Center for Internet (CIS), CIS Controls v7.1 Guide

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

State of Nevada

Information Security Committee

Standard

Document History

Revision	Effective Date	Change
A	6/04/2012	Initial release
B	12/26/2018	Renumbering (113 to S.4.03.01) and compliance to ADA standards
C	12/31/2020	Biennial review for alignment with CIS Controls v7.1, Implementation Group 1 (IG1)