State of Nevada
Information Security Committee

Standard

Document ID	Title	Revision	Effective Date	Page
S.6.10.01	Backup and Recovery Capabilities	D	12/31/2020	1 of 4

1.0 PURPOSE

This standard establishes the minimum requirements for information systems, information resources, and data backup procedures; backup schedules; and recovery plans, procedures, and tests.

2.0 SCOPE

This standard applies to all state agencies and authorized users meeting the criteria identified in the State Information Security Consolidated 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
Information Security Officer (ISO) Roles and Responsibilities, S.3.03.01
Data Sensitivity, S.3.02.01
IT Contingency Planning, S.3.09.01
Electronic Media Security, S.4.03.01

6.0 STANDARD

Each agency shall establish backup and recovery procedures and plans for information systems and applications, operating systems, and data processed and stored on IT resources, regardless of the IT platform being used.

6.1 Backups

Agencies, as the owners of the information, are responsible for ensuring the backup of their systems, applications, and data.

A. Hardware Technology Assets for Individual Use

Backup of data stored on hardware technology assets designated for individual use shall be the responsibility of the user. If an agency has an established policy regarding these issues, the agency policy supersedes this section.

B. Agency Servers

Backup of data stored on agency servers, including but not limited to information systems, data stores, and file servers, shall be the responsibility of the system administrator or person(s) assigned by the agency to maintain the server. If an agency

has an established policy regarding these issues, the agency policy supersedes this section.

C. Data Stored on Host IT Infrastructures

1. The agency and host IT service provider must specify in the written agreement, who will perform the backup of the application and data, and will provide a schedule for doing it. The host service provider of the IT infrastructure (e.g., the EITS-managed mainframe or the EITS server hosting environment) is responsible, at the minimum, for ensuring the backup and recovery of the operating systems.

2. The owners of the applications and data processed or stored on a host IT infrastructure, are responsible for coordinating, scheduling, and ensuring that:

   a. appropriate backups are accomplished, and

   b. appropriate backup and recovery plans, procedures, retention schedules, and testing are accomplished and documented.

3. Agency management or their designee shall periodically review and ensure that appropriate, proper backups are being made.

4. Frequency of backups shall be based on the criticality and sensitivity of the data along with the acceptable length of non-availability time for the IT resource and data. The frequency of the backup shall be documented in a backup schedule attached to the backup procedures.

5. Multiple generations of the backups shall be maintained to ensure recovery should any of the backups not recover properly, with at least one of those backups stored off-site.

6. Backup logs, backup reports, or other backup audit trails shall be maintained to track backup media; the information, data, or files backed up on the media, the date and time of the backup, and the successful completion of the backup.

6.2 Recovery

The procedures required for recovering from any incident creating the non-availability of a system, application or data will depend on the nature of the problem and the backup measures that have been taken.

A. Recovery procedures for each IT system, application and associated data shall be documented to define, in detail, the steps to accomplish the recovery from the appropriate backup. The documentation shall cover:

1. Identification of the system, application, or data to be recovered.

2. Identification and contact information of the primary and secondary staff responsible to accomplish the recovery.

3. Location of backup.

4. Specific step-by-step instructions for accomplishing the recovery.

5. Test procedures to take to ensure recovery was successful before declaring recovery complete and beginning of normal processing.

B. At least one copy of recovery procedures shall be maintained off-site.

C. Recovery procedures shall be revised upon any changes to the operating and storage environment of the systems, applications, or data.

D. Recovery procedures shall include, or at a minimum identify the location of, diagrams that provide network connectivity, system architecture, system setup, and other information that may be necessary to fully recover any particular system, application or data.

E. Agency management and both the primary and secondary person responsible for the recovery of any agency system, application, or data shall be familiar with and periodically review recovery procedures for clarity and identification of required revisions and responsibilities. Agency management shall maintain documentation indicating the responsible parties have continued to review the procedures.

6.3 IT Contingency Testing

A. Backup and recovery procedures shall be tested at least semi-annually or more frequently for critical mission systems, applications, and data. If a system restore is done, that restoration will count as a test but must be documented.

B. Testing of backups and recovery of systems, applications, and data can be accomplished at separate intervals.

C. Test plans shall be documented for each area (system, application, and data) of the backup and recovery effort. The test plan shall include test schedules and define if the test is for testing the backup procedures or recovery procedures of the system, application, or data, or a combination of all areas of both procedures. The plan shall specifically address the scope of the test and anticipated results.

D. Test results shall be documented. Test results that identify areas that need to be revised or that were unsuccessful shall be identified in the Test Result Report and required corrective actions identified with timeline for completion of corrective actions.

E. Test results shall be provided to the agency management for review and sign-off.

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 Security (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

Document History

Revision	Effective Date	Change
A	6/12/2003	Initial release
B	8/20/2014	OIS biennial review, replaces standard 4.32
C	12/26/2018	Renumbering (132 to S.4.04.01) and compliance to ADA standards.
D	12/31/2020	Biennial review for alignment with CIS Controls v7.1, Implementation Group 1 (IG1). Renumber from S.4.03.01 to S.6.10.01, as the standard purpose fully aligns with CIS Control 10 Data Recovery Capabilities.