



State of Nevada

State Information Technology Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
4.32	A	Data and System Backup and Recovery	6/12/03	1 of 4

1.0 PURPOSE

This standard establishes the requirement for IT system, application and data backup procedures, schedules and recovery plans, procedures and tests.

Information stored and processed on IT systems is vulnerable to degradation, accidental or intentional corruption or deletion, hardware/software failures and natural or man-made disasters. Backup and recovery procedures and plans are essential to ensuring recovery of information and the ability to continue IT support of critical business functions.

2.0 SCOPE

This standard applies to all state agencies meeting the requirements identified in the State IT Security Policy, Section 2.0 Scope.

3.0 EFFECTIVE DATES

The requirements of this standard are effective 90 days after sign-off by the Governor or his designee.

4.0 RESPONSIBILITIES

The agency head has the responsibility to ensure implementation and compliance to this standard.

5.0 RELATED DOCUMENTS

State IT Security Policy, 4.02
State Information Security Officer (ISO) Roles and Responsibilities, 4.03
IT Contingency Planning, 4.07
Data Sensitivity, 4.31

6.0 STANDARD

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

1. BACKUP STANDARDS

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

A. **MICROCOMPUTERS:** Backup of data stored on hard drives of microcomputers shall be the responsibility of the user. If an agency has an established policy regarding these issues, the agency policy supercedes this section.



State of Nevada

State Information Technology Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
4.32	A	Data and System Backup and Recovery	6/12/03	2 of 4

B. AGENCY RESIDENT SERVERS: Backup of data stored on agency 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 supercedes this section.

C. DATA STORED ON HOST IT INFRASTRUCTURES:

- 1) The agency and host provider must specify in the written agreement, who will perform the backup of the application and database and provide a schedule for doing it. The Host service provider of the IT infrastructure (example DoIT mainframe or Server Farm) is responsible, at the minimum, for ensuring the backup and recovery of the operating systems.
- 2) The owner of the applications and/or data processed and/or stored on a host IT infrastructure, is responsible for coordinating, scheduling and ensuring that appropriate backups are accomplished and 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 of 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 and at least one of those backups stored off-site.
- 6) Agencies not having media management systems shall ensure backup media has proper labeling, providing, at a minimum, the date of the backup, person accomplishing the backup, and identification of the system.
- 7) Backup logs shall be maintained to track backup media, files backed up on the media, data and time of the backup.

2. RECOVERY STANDARDS

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

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



State of Nevada

State Information Technology Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
4.32	A	Data and System Backup and Recovery	6/12/03	3 of 4

- 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 provides 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, identification of required revisions and responsibilities. Agency management shall maintain documentation indicating the responsible parties have continued to review the procedures.
3. **TESTING STANDARDS**
- 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) 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, data or a combination of all areas or 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 of completion of corrective actions.
- E. Test results shall be provided to the agency management for review and sign-off.



State of Nevada

State Information Technology Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
4.32	A	Data and System Backup and Recovery	6/12/03	4 of 4

7.0 DEFINITIONS/BACKGROUND

None

8.0 EXCEPTIONS/OTHER ISSUES

Requests for exception to the requirements of this IT Security Standard must be documented, provided to and approved by the State IT Security Committee and Chief Information Officer (CIO).

<i>Approved By</i>		
Title	Signature	Date
State IT Security Committee Chair	Signature on File	06/12/2003
NV IT Operations Committee Chair	Signature on File	06/12/2003
Governor/Governor's Representative	Signature on File	06/17/2003

<i>Document History</i>		
Revision	Date	Change
A	6/12/03	Initial release.