State of Nevada
Information Security Committee

Standard

Document ID	Title	Revision	Effective Date	Page
S.3.09.01	IT Contingency Planning	C	8/20/2014	1 of 3

1.0 PURPOSE

This standard establishes the minimum Information Technology (IT) Contingency Planning standard for an agency's mission critical information and the IT resources that support the critical mission of the agency.

Each agency must be able to continue to provide mission-critical services that are supported by IT resources should a situation occur that renders the IT resources inaccessible due to a system or application malfunction or hardware failure.

For the purpose of this policy "contingency planning" includes, but is not limited to, the documentation, plans, and policies and procedures required to restore mission-critical IT functions to include mainframe, mini-computers, servers, microcomputers, voice and data communications services, applications systems and related data.

2.0 SCOPE

This standard applies to all state agencies meeting the requirements identified in the State Information Security Consolidated Policy, Section 1.1, 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

6.0 STANDARD

6.1 Each agency shall develop, maintain and test IT Contingency Plans.

6.2 IT Contingency Plans shall contain sufficient information and instruction to enable the agency management to assure the agency's ability to continue its critical business services and operations, including those used by branch or remote offices.

6.3 Agencies that use computer or telecommunication services from either other governmental entities or commercial sources shall integrate and coordinate IT Contingency Plans, including off-site storage of data.

6.4 Agencies shall update IT Contingency Plans at least annually and/or following any significant change to the computing or telecommunications environment or critical function needs. Directors or identified agency heads shall review and approve agency new and revised plans.

6.5 Agencies shall identify and train appropriate employees to execute the IT Contingency Plans to include making employees aware of the need, existence of the agency IT Contingency Plan, along with the employees' responsibilities, and training the recovery team members to perform the procedures defined in the plan.

6.6 Agencies shall test the IT Contingency Plans and document the results. The type and extent of testing shall be dependent on the criticality of the function being supported by the IT resources. Agencies shall correct or establish a mitigation plan for correcting any deficiencies revealed by the test. The test results and mitigation plan shall be reviewed and approved by the agency head and provided to the State IT Security Committee Chair no later than January 15 of each year.

7.0 DEFINITIONS

Contingency Plans are related to, but do not take the place of, other types of plans. These plans are listed below, with the differences between plans addressed:

Risk Management Plan/Strategy: A Risk Management Plan identifies risks facing an agency and plans to mitigate those risks. Contingency Plans for IT resources are one component of an agency's risk strategy and thus should be consistent with the philosophy and goals of the overall risk management plan. However, Contingency Plans for IT resources are narrower in scope, dealing only with IT resources. An agency risk strategy is broader in scope, including abatements for risks in all resource categories such as staff, facilities, etc.

Disaster Recovery Plans: A Disaster Recovery Plan covers procedures for resuming agency functions in the case of a catastrophe. This type of planning assumes that few or none of the agency's normal operations can function. Contingency planning is similar to disaster planning, with two major differences. First, contingency planning does not assume the source of the failure, only the steps needed to resume normal operations. Secondly, contingency plans do not preclude the use of agency resources (e.g., facilities) that may not be available in the case of a true disaster.

Business Resumption Plans: A Business Resumption Plan covers the procedures needed to bring the agency back to normal business operations following a major disaster or business interruption. Contingency Plans address the recovery and resumption to normal operations of critical functions of the agency supported by IT resources. Whereas, a Business Resumption Plan addresses the resumption of business for the entire agency to include facilities, staff, etc.

Mitigation Plans: A Mitigation Plan describes what corrective measures need to be taken as a result of testing the contingency plan, the actions required to correct the weaknesses and a schedule to accomplish the corrective actions to include resource requirements.

8.0 RESOURCES

National Institute of Standards and Technology (NIST) Special Publication 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems, dated May 2010

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	1/30/2014
State Chief Information Security Officer (CISO)	Signature on File	8/20/2014
State Chief Information Officer (CIO)	Signature on File	8/20/2014

Document History

Revision	Effective Date	Change
A	4/11/2002	Initial release
B	8/20/2014	OIS biennial review, replaces standard 4.07
C	12/26/2018	Renumbering (125 to S.3.09.01) and compliance to ADA standards.