

Planning for IT Disaster Recovery and Business Resumption

Purpose: Ensure that information technology (IT) resource investments made by agencies of the executive and judicial branches of state government are protected against service interruptions, including large scale disasters, by the development, implementation, and testing of disaster recovery/business resumption (DR/BR) plans.

Effective Date: October 1, 2011

See Also: [Planning for Disaster Recovery and Business Resumption Standards \(151.10\)](#)
[Planning for Disaster Recovery and Business Resumption Guidelines](#)

POLICY STATEMENT

1. Each agency will develop disaster recovery/business resumption plans.

- 1.1. Agencies dependent on voice telecommunications, data telecommunications, video telecommunications, or computer services for carrying out their missions must develop disaster recovery/business resumption plans.
- 1.2. Agencies that purchase computer services or telecommunications services from other state agencies or commercial concerns will integrate their disaster recovery/business resumption plans, including off-site storage of data, with the service providers' plans.

2. Each agency will maintain and update disaster recovery/business resumption plans annually.

- 2.1. Agencies will also update disaster recovery/business resumption plans following any significant change to their computing or telecommunications environment.

3. Each agency will test disaster recovery/business resumption plans annually.

- 3.1. Agencies will correct any deficiencies revealed by the test. The type and extent of testing adopted by an agency will depend on:
 - Criticality of agency business functions.
 - Cost of executing the test plan.
 - Budget availability.
 - Complexity of information system and components.

4. Each agency will train their employees to execute the recovery plans. Training will consist of:

- Making employees aware of the need for a disaster recovery/business resumption plan.
- Informing all employees of the existence of the plan and providing procedures to follow in the event of an emergency.
- Training all personnel with responsibilities identified in the plan to perform the disaster recovery/business resumption procedures.

- Providing the opportunity for recovery teams to practice disaster recovery/business resumption skills.

5. Each agency will annually certify the updating and testing of the disaster recovery/business resumption plan.

5.1. An annual disaster recovery/business resumption plan confirmation letter must be included in the agency IT portfolio and submitted to the OCIO by August 31 of each year. By way of this letter, the head of each agency confirms to the Board that a disaster recovery/business resumption plan has been reviewed, updated, and tested.

6. The State Auditor may audit disaster recovery/business resumption plans and tests for compliance with policy and standards.

RESPONSIBILITIES

Chief Information Officer (or designee)

- Interpret the policy.
- Ensure policy content is kept current.
- Recommend updates to this policy and related resources as needed.

Technology Services Board (TSB)

- Review and approve major policy changes.

Agency Heads

- Responsible and accountable for its own disaster recovery/business resumption program.
- Maintain, update, and test disaster recovery plans annually.
- Adequately train staff to carry out disaster recovery plans.
- Certify updating and testing in annual letter to the OCIO.

DEFINITIONS

Disaster recovery/business resumption. Includes, but is not limited to, the documentation, plans, policies, and procedures that are required to restore normal operation to a state agency impacted by man-made or natural outages or disasters. The three principal goals of disaster recovery/business resumption planning are to:

- Save data.
- Save hardware, software, and facilities.
- Resume critical processes and restore data.

RELATED LAWS AND OTHER RESOURCES

[National Association of Chief Information Officers: IT Disaster Recovery and Business Continuity Tool-kit](#)

REVISION HISTORY

Date	Action taken
October 2011	Policy reformatted for migration to Office of Chief Information Officer. Added NASCIO toolkit reference.
April 2002	
July 1993	Policy adopted.

CONTACT INFORMATION

For questions about this policy, please contact your OCIO Information Technology Consultant.

APPROVING AUTHORITY

Chief Information Officer
Chair, Technology Services Board

Date