



Information Technology Services Policy Manual

18.05 Business Continuity Management

Purpose: To ensure that the appropriate level of business continuity management is in place to sustain the operation of ITS critical business services following a major disaster or emergency. To enable ITS to provide information technology support services to State government agencies with minimal disruption due to disasters or unforeseen events that would impact the agency's ability to service the citizens of North Carolina.

Reference: G.S. §147-33.89.

For More Information: Contact ITS Security Office, Business Continuity Management Program.

POLICY STATEMENT

ITS, under the direction of the ITS Business Continuity Management Program, shall maintain and test a business continuity program to support ITS operations and those operations that ITS operates on the behalf of its customers.

PROCEDURE

A management team composed of representatives from all ITS organizational areas has the primary leadership responsibility to identify risks and to determine what impact these risks have to business operations. The management team shall plan for business continuity based on these risks and document recovery strategies and procedures in a defined business recovery plan that is reviewed, approved, and updated on an annual basis. The plan includes all ITS divisions: business, technology and operational support because all ITS divisions perform functions critical to sustaining ITS service delivery.

Responsibilities of ITS managers/information owners include but are not limited to:

- Identification and prioritization of critical business processes.

- Regular assessment of the potential impact of various types of unforeseen events/disasters.
- Definition of responsibilities and emergency arrangements.
- Documentation of all procedures and responsibilities.
- Communication of business continuity and recovery plans to all necessary individuals.
- Regular testing of business continuity and recovery plans.
- Regular review of business continuity and recovery plans to ensure they are correct, complete and up-to-date.

The specific rules and procedures guiding the responsibilities and the actions to be taken in the event of a disaster are specified in the ITS Business Recovery Plan. The ITS Business Recovery Plan is assembled from the individual section plans under the direction of the ITS Business Continuity Management Program. In general, the ITS business recovery plan shall include the following types of activities.

- Activation of the ITS Business Recovery Plan and the notification of all responsible individuals (team leaders).
- Damage assessment team with recommendations to management regarding the extent of the damage and whether the facilities can be used safely in a reasonable amount of time or whether the hot site should be notified.
- Disaster declaration with activation of the ITS Business Recovery Plan.
- Measures to ensure the health and safety of all ITS employees and to recover the information systems once the employees' needs are satisfied. To assist with employee concerns, a team of individuals with the necessary skills in evacuation plans, emergency aid centers (like Red Cross, etc.), insurance claims, and any other concern which the employee feels is important to them and their families must be available if requested.
- Assignment of each ITS employee to a business recovery team. Each employee must understand his/her vital part of the recovery process.
- Procedures to declare a disaster and activate the hot site and restore the computer system and statewide network within 48 hours. The ITS technical team restores the ITS infrastructure environment.
- Communication plans to notify agencies of system availability. It is an agency responsibility to restore critical agency-owned applications.

- Application restoration program based on a criticality-ranking scheme of agency rankings and statewide needs.
- Plans for returning to the ITS data center from the hot site to resume normal business operations

ANNUAL REVIEW

The ITS Business Recovery Plan shall be reviewed based on a defined review process where managers shall submit their plans in June to the Business Continuity Management Program that shall submit the entire plan to the State Chief Information Officer for his/her signoff.

Effective Date: July 1, 1999

Approval Date: July 1, 1999

Revision Dates: September 12, 2000; April 9, 2003; March 30, 2004

§ 147-33.89. Business continuity planning.

(a) Each State agency shall develop and continually review and update as necessary a business and disaster recovery plan with respect to information technology. Each agency shall establish a disaster recovery planning team to develop the disaster recovery plan and to administer implementation of the plan. In developing the plan, the disaster recovery planning team shall do all of the following:

- (1) Consider the organizational, managerial, and technical environments in which the disaster recovery plan must be implemented.
- (2) Assess the types and likely parameters of disasters most likely to occur and the resultant impacts on the agency's ability to perform its mission.
- (3) List protective measures to be implemented in anticipation of a natural or man-made disaster.

(b) Each State agency shall submit its disaster recovery plan on an annual basis to the Information Resource Management Commission and the State Chief Information Officer."