NJ Office of Information Technology
Chris Christie, Governor
E. Steven Emanuel, Chief Technology Officer

P.O. Box 212
300 Riverview Plaza
Trenton, NJ 08625-0212

www.nj.gov/it/ps/

STATE OF NEW JERSEY IT CIRCULAR

Title: 195 – Contingency Planning Policy

NO:	SUPERSEDES:
14-31-NJOIT	N/A
LAST REVIEWED: October 24, 2014	**DATE PUBLISHED:** October 24, 2014
VERSION: 1.0	**EFFECTIVE DATE:** Date of Signature
FOR INFORMATION CONTACT: Office of Policy and Planning	

ATTN: Directors of Administration and Agency IT Managers

I. PURPOSE

The reliability and timely availability of electronic records and system applications are critical to the State of New Jersey's operations. The purpose of this policy is to describe the actions necessary when an unplanned event renders critical Information Technology (IT) systems and data unavailable. The goals are to restore and recover these IT systems and data properly and quickly. Contingency planning is designed to ensure continued operations while maintaining necessary levels of security. Planning and testing provide a foundation for a systematic and orderly resumption of all computing services within an agency after a disaster strikes.

II. AUTHORITY

This policy is established under the authority of the State of New Jersey. N.J.S.A. 52:18a-230 b. This policy defines New Jersey Office of Information Technology's (NJOIT) role with regard to technology within the Executive Branch community of State Government.

The New Jersey Office of Information Technology (NJOIT) reserves the right to change or amend this circular.

III. SCOPE

This policy applies to all State of New Jersey Departments, Agencies, State Authorities, "in but not of" entities, their employees, contractors, consultants, temporary employees, and other workers including all personnel who are tasked with the protection of the State of New Jersey resources and the Next Generation Services Network (NGSN).

IV. DEFINITIONS

Please refer to the Statewide Policy Glossary at http://www.nj.gov/it/ps/glossary/.

V. POLICY

Each Agency must meet the following requirements for developing a contingency plan that will take effect in the event of a disastrous reduction or loss of IT service to employees and clients:

A. Perform a Business Impact Analysis (BIA) for all systems to acquire an understanding of the potential risks that may affect critical business functions (http://www.nj.gov/it/reviews/forms/0104_Business_Impact_Analysis_Survey.pdf).

B. Determine the required availability (acceptable downtime) of all systems and networks and use the information both to create the contingency plan and develop a backup system.

C. Store backup media, documentation and other IT resources necessary to recover or resume IT processing at an off-site location. Backup procedures must provide the necessary data for recovery while minimizing data loss. The procedures will be included in the Contingency Plan.

D. Develop, maintain, and test a Contingency Plan for the critical systems identified in the BIA. The Contingency Plan is to describe the process for assuring the agency's ability to continue the critical business services and operations of each agency system, including systems used by branch or remote offices. The Contingency Plan must include:

1. Identification of key personnel with roles, responsibilities and 24/7 contact information.

2. Identification and description of teams necessary to execute the plan for the system. Designation of staff for the following teams should be considered:

a) System Contingency Coordinator.

b) Damage Assessment Team.

c) System Recovery Team.

d) Communications Team.

e) Operations Team.

f) Computer Incident Response Team.

g) Procurement Team.

3. Contact information of Vendors and Customers.

4. The Three Stages of Action following system disruption.

a) Activation and Notification – Activities to notify recovery personnel, conduct an outage assessment, and activate the plan.

b) Recovery – Recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or new alternate location.

c) Reconstitution – Procedures for validating successful recovery and deactivation of the plan.

5. A description of the response process to an incident, including expectations of the time needed to complete the response.

6. Detailed recovery execution strategies, processes, and procedures for restoring systems to production.

7. Documentation of each critical system including:

a) Name of Function / Application.

b) Purpose / Business Process of the system.

c) Hardware.

d) Operating System.

e) Application(s).

f) Supporting network infrastructure and communications.

g) Identity of person responsible for system restoration.

8. The conditions that might activate the plan (e.g. facilities, hardware or software unavailability for more than 24 hours). The System's Contingency Plan may be activated independent of other organizational plans such as a Disaster Recovery Plan (DRP) or a Continuity of Operations Plan (COOP).

9. A description of current system back-up procedures.

10. A description of back-up storage location.

11. An outline of a distribution strategy that will ensure all applicable personnel are informed of the contingency approach in the plan.

E. Perform annual training and testing of the contingency plan to ensure all critical participants know their roles and responsibilities and to facilitate any needed corrections to the plan. Training and testing can be performed simultaneously. The types of test are as follows:

1. Call tree verification for low-level availability systems.

2. Tabletop test for most systems.

3. Failover test of critical availability systems to a hot, mirrored backup system.

VI. ROLES AND RESPONSIBILITIES

A. The Statewide Office of Information Security.

1. Will work with IT Directors and designated Security Officers and the agency programs to review and update this policy and documentation.

B. Departments and Agencies.

1. The IT Directors shall coordinate with the responsibilities of the agency programs Continuity Manager in support of their individual Contingency Plans.

2. The IT Directors shall coordinate their individual Contingency Plan with the State of New Jersey's Continuity of Operations Plan.

3. IT Directors must coordinate this policy with 11-02-NJOIT *190 – Information Security Incident Management Policy.*

VII. EXCEPTIONS AND NON-COMPLIANCE

Departments and Agencies shall comply with this policy within 90 days of its effective date.

Requests for exceptions for non-compliance with this policy shall be processed in accordance with Statewide IT Circular 08-02-NJOIT *111 – Information Security Managing Exceptions*.

Signature on File — *10/28/2014*

E. STEVEN EMANUEL — **DATE**
Chief Technology Officer-NJ Office of Information Technology
State Chief Information Officer