



<b>State of New Jersey IT Circular</b>  <b>Title: Use of Statewide Disaster Recovery Facilities</b>	<b>NO:</b> <b>07-10-NJOIT</b>	<b>SUPERCEDES:</b> n/a
	<b>DATE PUBLISHED:</b> 06-11-2007	
	<b>VERSION:</b> 1.0	<b>EFFECTIVE DATE:</b> 06-11-2007
	<b>FOR INFORMATION CONTACT:</b> Elizabeth Caldwell, Office of Policy and Planning (609) 633-0429	

ATTN: Directors of Administration and Agency IT Managers

## I. PURPOSE

A. This policy defines specific requirements for placing equipment and/or application environments at the New Jersey's disaster recovery facilities in support of mission critical business functions:

1. Establishes a directive for the use of disaster recovery facilities; and
2. Provides direction regarding the requirements for establishing disaster recovery capability at disaster recovery facilities.

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

## II. AUTHORITY

This policy is established under the authority of State of New Jersey P.L.2007.c.56.

## III. SCOPE

This policy in its entirety applies to the executive branch IT personnel who are responsible for building and/or developing information technology environments that support disaster recovery for critical business functions as defined in business impact analysis (BIA) reports.

## IV. DEFINITIONS

A. BIA

Refers to Business Impact Analysis, which determines the financial, or functional, loss over time when information systems are lost, or down, due to a disaster.

**B. Disaster Recovery / Continuity of Operations (COOP)**

Are commonly used terms referring to the steps required to recover business functions and service following either a disaster or other event resulting in a long term disruption of business activity.

**C. Disaster**

Is any sudden or unplanned calamitous event that causes a significant disruption in information systems and/or telecommunications systems or business function that significantly affects the operation of an organization.

**D. Recover Time Objective (RTO)**

Is the period of time within which systems, applications, or functions must be recovered after an outage (e.g. one business day). RTO's are often used as the basis for the development of recovery strategies, and as a determinant as to whether or not to implement the recovery strategies during a disaster situation.

**V. POLICY**

**A. Agency participation and access to the disaster recovery facility:**

1. Applications and hardware platforms must support mission critical functions, as defined in the agency COOP plan and/or BIA;
2. Applications and hardware platforms must be compatible with currently installed and supported infrastructure within the disaster recovery facility; and
3. Participants must conform to defined facilities management procedures that will be made available at the time of engagement.

**B. Any organization placing equipment and/or application environments at a disaster recovery facility, at a minimum must insure adequate documentation is provided, that includes:**

1. Written procedures for performing recovery of the application environment;

2. Drawings that depict the environment and dependencies on related systems;
  3. Any reference material required to support the stated recovery time objective (RTO) (Attachment #1); and
  4. Documentation must include environmental requirements (power usage, rack space and other footprint requirements).
- C. The standard NJOIT Change Management procedures will be used for installing or modifying equipment and/or applications hosted at the disaster recovery facility.
- D. A written request must be submitted to the Statewide Disaster Recovery & Planning Officer for a new application environment to be considered for installation within a statewide disaster recovery facility.
1. A minimum of eight weeks lead-time should be provided to the facility Operations Manager for planning installation.
  2. A minimum of eight weeks lead-time should be provided to the facility Operations Manager to plan the testing of any application or equipment.
  3. For new installations, the request must include the referenced information listed in Section V.B. Facilitation and guidance are available to support new installations from the Statewide Disaster Recovery & Planning organization.

## VI. RESPONSIBILITIES

### A. Chief Technology Officer, Deputy Chief Technology Officers and Agency Senior IT Leaders

1. Responsible for ensuring that OIT and Agency staff are aware and adheres to this policy.
2. Responsible for ensuring all NJOIT and using departments/agencies cooperate in the execution of the requirements of this policy.

### B. Statewide Disaster Recovery & Planning Officer

Recommends to CTO approval/denial of the written request for a new application environment to be considered for installation within a statewide disaster recovery facility.

**C. Office of Business Continuity and Disaster Recovery**

Is responsible for educating users of the OARS facility about this policy and monitoring compliance.

**D. Directors, Business Unit Managers and Supervisors**


Are responsible for insuring requirements of this policy are fulfilled by the respective organizational components and that staff cooperate with the Office of Business Continuity and Disaster Recovery in the execution of its responsibilities in regard to this policy.

**VII. EXCEPTIONS**

Any exceptions to this policy must obtain written prior approval of the CTO or their designee.

**VIII. NON COMPLIANCE**

1. Agencies choosing not to comply with this policy will not be permitted to host environments at a statewide disaster recovery facility.
2. Agencies found to be in violation of P.L.2007.c.56 risk the loss of future capital and/or operating funds reserved for this purpose.



---

Adel Ebeid, Chief Technology Officer  
NJ Office of Information Technology