NJ OFFICE OF INFORMATION TECHNOLOGY
Philip D. Murphy, Governor
Odysseus Marcopolus, Chief Operating Officer
P.O. Box 212
300 Riverview Plaza
Trenton, NJ 08625-0212
www.tech.nj.gov

STATE OF NEW JERSEY TECHNOLOGY CIRCULAR 164 – Backup and Restore Policy	**POLICY NO:** 15-04-NJOIT	
	SUPERSEDES: NEW	**EFFECTIVE DATE:** 01/22/2015
	VERSION: 1.0	**LAST REVIEWED:** 01/22/2015

ATTN: Directors of Administration and Agency IT Managers

1 PURPOSE

Information stored and processed on Information Technology (IT) systems is vulnerable to accidental degradation, intentional corruption or deletion, hardware/software failures, and natural or man-made disasters. A Backup and Restore policy is essential to ensuring recovery of information and the ability to continue IT support of critical State business functions. System backups also are an essential component of contingency planning strategies. Backups enable IT support personnel to quickly and reliably recover essential data and software in case of events such as natural or environmental disasters, system or application failures, sabotage, data/system integrity errors and/or system operations errors.

2 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.

3 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.

4 DEFINITIONS

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

5 POLICY

The following requirements provide a policy for backup and restoration of the State's systems in the event of a reduction of service to employees and clients. Each Agency shall:

5.1.1 Ensure the type of backup performed will be according to the criticality of the data as determined in 08-04-S1-NJOIT, *130-01 Asset Classification and Control Standard.* The following types of backups can be utilized:

5.1.1.1 Full – Includes files whether they have been changed or not;

5.1.1.2 Differential – Includes all files changed since the last full backup, whether they have been changed since the last backup operation or not;

5.1.1.3 Incremental – Includes only those files that have changed since the last backup operation of any kind.

5.1.2 Ensure all data in backups are secured according to the data classification, including requirements such as data isolation and/or segregation.

5.1.3 Develop procedures for backup, storage and restoration of all systems data and ensure that the procedures will be followed at a frequency as determined by the Agency. These procedures should be included in the agency's contingency plan.

5.1.4 Ensure that the storage and location of backup media shall be in a physically and environmentally secure location remote from the main processing site and adequately labeled to ensure proper handling and prompt identification.

5.1.5 Ensure that the transport of backup media to remote locations will be performed only by authorized personnel.

5.1.6 Ensure that backup media and restoration procedures are routinely tested to ensure that the State can restore and recover information; that backup procedures are correct, and that restored information has not been compromised.

5.1.7 Ensure that system owners are notified when backups have not been performed according to schedule or if there is a failure during testing of backups.

5.1.8 Determine a retention period for all backup media according to the criticality of the data.

5.1.9 Maintain backup logs to track backup media, files backed up on the media, data and time of the backup.

6 ROLES AND RESPONSIBILITIES

6.1.1 The Statewide Office of Information Security

6.1.1.1 Will work with IT Directors, designated Security Officers and Business to review and update this policy and documentation.

6.1.2 Departments and Agencies

6.1.2.1 The IT Directors shall coordinate with the responsibilities of the Business Continuity Manager in support of their individual Backup and Restoration requirements and storage locations.

6.1.2.2 The IT Directors shall review and approve backup and restoration procedures and ensure testing occurs on a regular basis.

7 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.*