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 168 – Change Management Policy	**POLICY NO:** 14-09-NJOIT	
	SUPERSEDES: NEW	**EFFECTIVE DATE:** 01/07/2014
	VERSION: 1.0	**LAST REVIEWED:** 01/07/2014

ATTN: Directors of Administration and Agency IT Managers

1 PURPOSE

The purpose of this policy is to manage the effects of changes or differences in configurations of State of New Jersey information systems or networks (including hardware, software, infrastructure and documentation). Change management allows system owners to handle changes in a controlled, predictable and repeatable manner and assess, identify and minimize the risks to operations and security prior to implementation.

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 the 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, "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 Garden State Network.

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 managing the configuration and change of the State of New Jersey's resources:

5.1.1 A baseline configuration and inventory shall be created and maintained for each configuration item of a system.

5.1.2 All default system administrator passwords must be changed before a system is base lined.

5.1.3 All security settings of components shall be configured to the most restrictive mode consistent with operational requirements.

5.1.4 Access to changes or settings of component configuration will be restricted to authorized personnel.

5.1.5 Each agency will establish a review process for change requests and decide to approve or deny a change. The process will ensure each change is documented and recorded in a central change management repository or system. Documentation of the change request can come from various sources:

5.1.5.1 Initial change request which may include:

5.1.5.1.1 Provisions for emergency changes

5.1.5.1.2 Version control for all updates

5.1.5.1.3 Installation without business interruption

5.1.5.1.4 Allowances for rollback as a result of anticipated possible failure of the change.

5.1.5.1.5 System upgrades and patch management.

5.1.5.2 Impact analysis of change request including network, users, security and interface with other systems.

5.1.5.3 Approval or rejection of the change.

5.1.5.4 Updated configuration documentation.

5.1.5.5 Successful test of change before allowed into production environment.

5.1.5.6 Implementation of change by authorized personnel only.

5.1.6 The review process should be evaluated at least annually.

6 ROLES AND RESPONSIBILITIES

6.1.1 The State of New Jersey Government Entities

6.1.1.1 Any department, agency, "in but not of" entity, requiring deviations from the standard configuration must formally request these changes and take responsibility to provide compensating controls to ensure the security of the State's asset or system.

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.*