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 115 – Information Security Risk Management Policy	**POLICY NO:** 14-02-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 specify how the Executive Branch of New Jersey State Government will ensure that the State's information systems comply with applicable state and federal laws governing appropriate policies on information security, and to implement a risk management program that enhances the security of confidential, proprietary, and sensitive information.

2 AUTHORITY

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

The New Jersey Office of Information Technology reserves the right to change or amend this policy.

3 SCOPE

This policy applies to all State of New Jersey Departments, Agencies, "in but not of" entities, their employees, contractors, consultants, temporary workers, and others who develop and administer information systems and resources for those systems.

4 DEFINITIONS

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

5 POLICY

This policy outlines methodology for assessing, mitigating and evaluating security risks of the State of New Jersey's information assets. The goal is to ensure appropriate levels of confidentiality, integrity, and availability of State data. OIT has developed a well-structured risk assessment and management plan to help departments and/or agencies:

5.1.1 Determine security capabilities and controls necessary to better secure information technology systems that store, process, and/or transmit department and/or agency information.

5.1.2 Enable management to make well-informed decisions about risk management and related expenditures, and incorporate them into their information technology budgets.

5.1.3 Assist management in authorizing the use of information technology systems, based on supported documentation.

The risk management process will have three major components and the risk management plan will be a primary tool during the three phases of the process. The Office of Information Technology has a risk management plan that departments and/or agencies can reference and use to complete the three major components. OIT's Statewide Office of Information Security will provide a copy of the risk management plan upon request to authorized personnel.

6 PROCEDURE

6.1.1 Assessment

Immediately after the scope or definition of the system is defined and developed, the department and/or agency will complete a risk assessment to determine the extent and likelihood of potential threats and vulnerabilities, and the resulting risks associated with a system. The risks are documented using OIT's risk management remediation report template. The output of the risk assessment will help identify what controls and procedures should be used to mitigate risk.

6.1.2 Mitigation

The agency should prioritize the risks, and implement risk mitigation controls and procedures, taking into account costs and the likely effects of these controls and procedures on other parts of its operations and on State's infrastructure.

6.1.3 Evaluation

The department and/or agency will schedule periodic risk assessments and disaster recovery testing to adapt to changes in system components, security threats and statewide procedures and best practices.

7 RESPONSIBILITIES

7.1.1 Statewide Office of Information Security:

7.1.1.1 Provide oversight of the risk assessment and management plan, and guidance on the use of the plan and template.

7.1.1.2 Communicate to IT Directors and other management and personnel of known risks.

7.1.1.3 Provide risk remediation reports to IT Executive Management within OIT and Departments and/or Agencies when known risks have been identified.

7.1.1.4 Work with IT Directors and designated Security Officers to review and update this policy and documentation.

7.1.2 Departments and Agencies:

7.1.2.1 The IT Directors shall follow and support the risk assessment and management plan that falls under their area of control. This includes participating in identifying security risks, and then mitigating risks that have been identified.

7.1.2.2 Identify, document, mitigate and evaluate risks of all systems under their control.

8 EXCEPTIONS AND NON-COMPLIANCE

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

A compliance exception must be requested if there is an inability to comply with this policy because of a business reason or system constraint. Exceptions and non-compliance with this policy shall be managed in accordance with Policy 08-02-NJOIT, 111 – Information Security Managing Exceptions.