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 184 - Information Security Vulnerability Management Policy	**POLICY NO:** **12-04-NJOIT**	
	SUPERSEDES: NEW	**EFFECTIVE DATE:** 05/03/2012
	VERSION: 2.1	**LAST REVIEWED:** 12/11/2014

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 reduce the risk of threats or attacks to the State's information assets by proactively managing exploitable vulnerabilities.

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 employees, contractors, and others who develop, administer, and maintain information systems, networks, software applications and resources for New Jersey State Government, Office of Information Technology and their clients.

4 DEFINITIONS

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

5 POLICY

New Jersey has created an Information Security Vulnerability Management Program to ensure the protection of the State information assets. The goal is to identify and remediate vulnerabilities before attackers can exploit them.

The program will help the State assess information assets, document a repeatable remediation process, assist with regulatory compliance requirements, and determine responsibility and accountability for identifying and addressing vulnerabilities. The program also is designed to ensure that departments and agencies scan new information assets before deployment in a network and that IT staff have assessment tools available for ad hoc scanning or assessment needs.

Departments and Agencies must participate in the Information Security Vulnerability Management Program.

OIT has implemented the Information Security Vulnerability Management Program into its System Architecture Review (SAR) process. Departments and Agencies must plan and implement the Information Security Vulnerability Management Program into their System Development Life Cycle (SDLC).

As part of managing ongoing security threats to the State's Information Assets, Departments and Agencies must implement a Patch Management Program. The program must include a comprehensive methodology for identifying when patches are needed. The State is to apply patches in a timely manner to protect against the introduction of malicious software and other types of attacks.

6 RESPONSIBILITIES

6.1 Statewide Office of Information Security

The Statewide Office of Information Security personnel will provide oversight and day-to-day support of the Information Security Vulnerability Management Program. Statewide Office of Information Security personnel assigned to the Enterprise Vulnerability Management Program shall:

6.1.1 Ensure the availability of information security vulnerability management scanning services.

6.1.2 Manage the review and evaluation of risk and remediation challenges and provide recommendations to IT Management.

6.1.3 As vulnerabilities are identified, communicate the level or levels of risk posed by the vulnerabilities to IT Directors and other management and personnel.

6.1.4 Provide enterprise vulnerability reports to IT Executive Management within OIT and to participating Departments and/or Agencies on a regularly scheduled basis. Brief IT Executive Management regularly on the information program's activities, successes, and shortfalls.

6.2 Departments and Agencies

The IT Directors shall support the activities of the Information Security Vulnerability Management Program that fall under their area of control. This includes participating in enterprise and individual scanning, as well as the maintenance of their Patch Management processes.

6.2.1 IT Directors must review reports of vulnerabilities and their risk levels on a regularly scheduled basis.

6.2.2 IT Directors must ensure that identified vulnerabilities in systems under their control are remediated according to their levels of risk.

6.2.3 IT Directors shall participate in Information Security Vulnerability Management knowledge sharing between Departments and Agencies as appropriate.

7 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 any portion of this policy. Exceptions and noncompliance shall be managed in accordance with Policy 08-02-NJOIT, *111 - Information Security Managing Exceptions.*