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 176 – Information Security System Monitoring and User Review Policy	**POLICY NO:** **15-02-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

The objective of this policy is to ensure that the State assesses security controls and risks at a frequency sufficient to ensure the best possible protection for New Jersey's information assets.

2 AUTHORITY

This policy is established under the authority of the State of New Jersey. N.J.S.A. 52:18a-230 b. It 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 assets.

4 DEFINITIONS

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

5 POLICY

The monitoring of Information Security is a dynamic process. The State must manage this process so it can identify and respond quickly to new vulnerabilities, evolving threats, and the constantly changing enterprise architecture and operational environment.

State-wide monitoring cannot be efficiently achieved through manual or automated processes alone. A combination of strategies is necessary. Where manual processes exist, the processes must be repeatable and verifiable to enable consistent implementation. Automated processes, including the use of automated support tools (e.g., vulnerability scanning tools, network scanning devices, logging/auditing); can make the process of continuous monitoring more consistent and efficient.

5.1.1 The State has the right to monitor and filter enterprise systems.

5.1.2 The State shall provide fair notice of system monitoring using reminders or warning banners, reference 14-04-S1-NJOIT, *1703-01 Disclaimer Standard*.

5.1.3 State and non-State users shall be aware of and acknowledge their security responsibilities.

5.1.4 Network, operating system, and application administrators who have a security role, as appropriate, shall create, use, review, protect, and retain system audit logs and security tool data, and follow the 14-28-NJOIT, *202 – Asset Audit and Accountability Policy.*

5.1.5 Department and agencies will consolidate audit logs and forward events to a central department or agency's Security Incident Event Management (SIEM) system. The department or agency's SIEM will be integrated with the State's SIEM.

5.1.6 Department and agencies will outline the expectations of personnel assigned with system monitoring duties.

5.1.7 Departments and agencies will be notified when malicious events appear to be originating from their network segments.

6 RESPONSIBILITIES

6.1.1 Statewide Information Security Officer (SISO)

The SISO is responsible for the development and coordination of the Statewide Information Security Program and performs the following duties:

6.1.1.1 Oversees the system monitoring program and periodically assesses whether the program is implemented effectively.

6.1.1.2 Works with operational managers to implement a process for continuous monitoring and reporting of unauthorized activity. All security monitoring activities shall be approved by the SISO.

6.1.1.3 Develops and implements Security policies, standards and procedures.

6.1.1.4 Reviews requested exceptions to Security policies, standards and procedures.

6.1.1.5 Provides solutions, guidance and expertise in IT security.

6.1.1.6 Coordinates events and incidents in accordance with 11-02-NJOIT, 190-NJOIT - Information Security Incident Management Policy; 11-02-P1-NJOIT, 190-00-01 Information Security Incident Management Reporting Procedures; and 11-02-P2-NJOIT, 191 - Information Security Incident Management Response Procedures.

6.1.2 OIT Management

OIT managers are empowered and expected to terminate communications when activities from within a client agency jeopardize the proper functioning or security of State-owned or managed resources that support other client agencies. Actions to protect State assets and infrastructure and client operations shall take precedence over executive communications. The affected organization's CIO and the appropriate organizational chain shall be briefed when time permits on the events and actions taken during the emergency.

6.1.3 Office of EEO/AA/Ethics, Employee Relations or Human Resources

An agency's Office of EEO/AA/Ethics, Employee Relations or Human Resources shall take a significant role in all event/incident investigations that involve or might involve employees. For events/incidents that are or could be attributable to employees of other state departments/agencies, management will make the necessary notifications to their counterparts in the other departments/agencies.

Authorization to focus on a specific employee shall require senior management approval that has been coordinated with the agency's Employee Relations Office, Office of EEO/AA/Ethics and HR.

6.1.4 System and network administrators

System and network administrators shall review system audit logs for which they are responsible at least weekly.1 Priority for log reviews shall be given to systems known to contain confidential and/or personal information. Administrators shall report all findings of anomalous activity that may be security-relevant in accordance with Policy 11-02-NJOIT, *190 - NJOIT - Information Security Incident Management Reporting Policy*.

7 EXCEPTIONS AND NON-COMPLIANCE

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*.

[1] May also include application, database, and/or storage administrators as appropriate.