NJ OFFICE OF INFORMATION TECHNOLOGY
Chris Christie, Governor
Dave Weinstein, Chief Technology Officer

P.O. Box 212
300 Riverview Plaza
Trenton, NJ 08625-0212

www.tech.nj.gov

STATE OF NEW JERSEY TECHNOLOGY CIRCULAR 202 –Asset Audit and Accountability Policy	**POLICY NO:** 14-28-NJOIT	
	SUPERSEDES: NEW	**EFFECTIVE DATE:** 11/3/2014
	VERSION: 1.0	**LAST REVIEWED:** 11/3/2014

ATTN: Directors of Administration and Agency IT Directors

1 PURPOSE

Information security audits are a vital tool for governance and control of agency IT assets. IT security audits assist agencies in evaluating the adequacy and effectiveness of controls and procedures designed to protect State of New Jersey's information and IT systems. This policy provides assurance that the State's systems and assets are capable of generating usable audit records for specified events to enable after-the-fact traceability and investigation of security incidents.

Agencies are reminded that the management and retention of all records stored electronically are subject to the Treasury's "Division of Revenue and Enterprise Services Records Management's retention requirements.

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 system administrator personnel and others tasked with the protection of the State of New Jersey information and assets from unauthorized access or unusual activity.

4 DEFINITIONS

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

5 POLICY

Agencies shall implement a program for continuous monitoring and auditing of system use to detect unauthorized activity. All network components and computer systems used for agency operations must have the audit mechanism enabled and shall include logs to record specified audit events in accordance with *14-01-S1-NJOIT, 171-01 Minimum System Security and Protection Standards*. Additional audit activity will be periodic and\or event driven to assure compliance with internal policies, support the performance of internal investigations, and assist the management of information systems.

In order to audit and be accountable, agencies will:

5.1.1 Determine, based on risk, business needs and regulatory requirements, the events to be audited for the individual system.

5.1.2 Allocate sufficient audit record storage capacity to limit the possibility of the capacity being exceeded. Refer to NIST Special Publication 800-92 "Guide to Computer Security Log Management" (table 4.1) for guidance on local system log retention configuration options. The Auditing system should be configured to alert agency officials when 90% capacity is reached.

5.1.3 Determine the level of review, analysis and reporting, and provide adjustments based on the risk to operation. This could include employees suspected of misuse or violations that may have their computer activity logged for further action.

5.1.4 Centralize the review and analysis of audit records from multiple components within the system and from multiple systems with the agency.

5.1.5 Provide the ability for quarterly reports based on criteria requested by individual system owners.

5.1.6 Ensure that audit findings are reported to organization management for mitigation and corrective actions.

5.1.7 Ensure system time clocks are updated daily from the State's provided time source to confirm the validity of audit trails and certify any required evidence,

and the synchronized correct time must then be disseminated to all systems on an agency's network.

5.1.8 Provide adequate protection of audit records from unauthorized access or modification.

5.1.9 Ensure users of all systems shall have unique IDs to protect against an individual denying having performed a particular action.

5.1.10 Audit records shall be archived and retained for at least one year or based on state and federal requirements. Audit logs of remote-access activities shall be maintained for at least ninety (90) days.

5.1.11 System operations and system security administration shall be performed by different personnel.

5.1.12 Ensure that audit logging of any firewalls and other network perimeter access control systems are enabled.

5.1.13 Ensure that an audit trail of physical access to the computer area and State of New Jersey assets are maintained.

5.1.14 If supported, auditing features on wireless devices shall be enabled and the auditing information reviewed periodically by designated staff.

6 RESPONSIBILITIES

6.1.1 Statewide Office of Information Security

6.1.1.1 The SOIS is responsible for oversight of this policy.

6.1.2 Agencies

Each Agency has ultimate responsibility for the protection of its information from disclosure, loss, or misuse. As such, each agency must maintain a thorough audit of these assets, understand and manage risks associated with the use of these assets. Agencies must adhere to all information security policies and program functions. Agencies shall immediately notify the OIT's Statewide Office of Information Security of any information security issues, incidents, problems, or threats resulting from audit logging and reports in accordance with 11-02-NJOIT, *190 – Information Security Incident Management Policy*.

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.*

Signature on File *11/13/2014*

E. STEVEN EMANUEL **DATE**
Chief Technology Officer-NJ Office of Information Technology
State Chief Information Officer