NJ Office of Information Technology
Chris Christie, Governor
E. Steven Emanuel, Chief Technology Officer

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

www.nj.gov/it/ps/

STATE OF NEW JERSEY IT CIRCULAR

Title: 100 Information Security Program

NO:	SUPERSEDES:
08-01-NJOIT	N/A
LAST REVIEWED: January 21, 2016	**DATE PUBLISHED:** June 18, 2008
VERSION: 2.0	**EFFECTIVE DATE:** Date of Signature
FOR INFORMATION CONTACT: Office of Policy and Planning	

ATTN: Directors of Administration and Agency IT Managers

I. PURPOSE

The State of New Jersey is committed to protecting the information assets and resources of the state and its constituency. All State agencies have a responsibility of due diligence and due care to that commitment. Under that authority and in support of the commitment to protect information assets and resources, OIT maintains oversight for developing an Information Security Program to ensure the availability, integrity, and protect the confidentially of those information assets and resources within the Executive Branch of State Government.

The primary objectives of this Information Security Program are to:

A. Effectively manage risks associated with exposure or compromise of agency information assets.

B. Define and communicate responsibilities for performing information security duties.

C. Ensure the implementation of security controls, both technical and non-technical, across the enterprise.

D. Provide a framework for statewide security compliance efforts.

E. Increase the awareness and importance of information security in all state agencies.

II. 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.

III. SCOPE

This policy applies to all personnel including employees, temporary workers, volunteers, contractors, and those employed by contracted entities, and others who administer state information resources.

IV. POLICY

This policy establishes that the Statewide Information Security Officer (SISO) and the Statewide Office of Information Security are responsible for directing the Information Security Program and providing leadership and coordination of information security programs and services across the enterprise. This policy also establishes the responsibilities of Agencies in securing information assets and resources.

The Information Security Program will establish and ensure that:

A. Physical, technical, and administrative information security controls are implemented and maintained to protect the confidentiality, integrity, and availability of information and information resources within the state.

B. Statewide information security policies, standards, procedures, and any associated guidelines are developed, maintained and promulgated across the enterprise.

C. Legal, regulatory, and contractual requirements will be met in support of managing and protecting statewide information assets and resources.

D. Information Security awareness and training will be provided to all.

E. All employees will be held accountable for fulfilling their individual information Security responsibilities.

V. RESPONSIBILITIES

A. Chief Technology Officer

The CTO has ultimate authority and oversight for the approval, interpretation, implementation, and enforcement of all Information Security Program specifics.

B. 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:

1. Administer the program and periodically assesses whether the program is implemented effectively.

2. Develop and implement Security Policies, Standards and Procedures.

3. Review requested exceptions to Security Policies, Standards and Procedures.

4. Provide solutions, guidance and expertise in IT security.

5. Maintain awareness of security status of IT systems.

6. Communicate requirements of Information Security Policies and legislative mandates.

7. Implement Security Awareness program.

8. Respond to security incidents.

C. Agencies

Each Agency has ultimate responsibility for the protection of its information from disclosure, loss or misuse. As such, each agency must maintain thorough knowledge of these assets and understand and manage risks associated with the use of these assets. Agencies must adhere to all information security policies and program functions. Each agency shall designate an information security point of contact(s) to address program needs, participate in enterprise information security matters as well as interact with SISO as needed. Agencies shall immediately notify SISO of any information security issues requiring attention.

VI. EXCEPTIONS AND NON-COMPLIANCE

Failure to comply with this policy may result in disciplinary action.

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 Statewide IT Circular 08-02-NJOIT*, 111 – Information Security Managing Exceptions*.

Signature on File *1/21/2016*

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