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 180 – Security in Application Development Policy	**POLICY NO:** 14-08-NJOIT	
	SUPERSEDES: NEW	**EFFECTIVE DATE:** 01/07/2014
	VERSION: 1.0	**LAST REVIEWED:** 01/07/2014

ATTN: Directors of Administration and Agency IT Leaders

1 PURPOSE

The purpose of the Security in Application Development policy is to set business requirements that ensure that the State's approach to application development properly balances utility for users and other considerations with minimum required security requirements. The policy addresses security controls needed to ensure that the data processed by State applications is accurate and protected from misuse.

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/APPLICABILITY

This policy applies to the development of all State government applications. The principles described in this policy also apply to the development of applications provided by organizations outside the state.

4 DEFINITIONS

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

5 POLICY

All information technology services and systems developed or acquired by agencies shall have documented security specifications that include an analysis of security risks and recommended security controls as described in 14-01-NJOIT, *171 – Minimum System Security and Protection Policy*. A security plan shall also be required during the design phase of the software or system development life cycle, and will describe the administrative, physical, technical and systems controls to be used by the application and/or services.

During application development, all recommended security controls should be developed and implemented so that they are part of the system rather than added at completion. Security tools should be utilized in development to minimize potential vulnerabilities to application code as well as to the systems where the applications reside or with which the applications integrate.

State agencies shall evaluate the security history and standards of commercial application providers before purchasing their products. State agencies are ultimately responsible for the security of the products implemented and shall select and manage their vendors accordingly.

Outsourced development activities shall be structured and monitored to ensure that security controls used during development, testing, and deployment are equal to or more stringent than the security requirements that the State requires for internal application development.

Test environments should be separate from the production environment during development. Data used for testing cannot contain confidential or sensitive information. The State will consider the security implications and risks before making business decisions about applications.

6 RESPONSIBILITIES

6.1 Departments and Agencies

6.1.1 Information Technology Directors, Managers, and Supervisors shall ensure that the minimum security requirements standards are applied during development of applications under their control. IT Managers and Supervisors shall report any requests for exceptions or OIT approved exceptions to these minimum standards to their IT Director or designee.

6.2 State of New Jersey IT Administrators

6.2.1 All Administrators who prepare, administer, and maintain state applications shall ensure that the minimum security requirements standards are implemented on the application under their control. IT Administrators shall also be responsible for reporting unauthorized modification or circumvention of security controls to their IT Directors, Managers, and/or Supervisors.

6.3 Statewide Office of Information Security (SOIS)

6.3.1 The SOIS is responsible for oversight of this policy.

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 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.*