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 182 – System and Services Acquisition Policy	**POLICY NO:** 14-25-NJOIT	
	SUPERSEDES: NEW	**EFFECTIVE DATE:** 10/24/2014
	VERSION: 1.0	**LAST REVIEWED:** 10/24/2014

ATTN: Directors of Administration and Agency IT Managers

1 PURPOSE

The purpose of this policy is to establish a system and services acquisition process for information technology that ensures security for and manages the risks of the usage of third party products and service providers.

2 AUTHORITY

This policy is established under the authority of the State of New Jersey P.L.2007.c.56. This order defines New Jersey Office of Information Technology's role with regard to technology within the community of the Executive Branch 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 all State of New Jersey systems and equipment that are used to process, transmit, or store information. This policy also applies to all State personnel, including employees, temporary workers, volunteers, contractors, those employed by contracted entities, and others who administer enterprise information resources.

4 DEFINITIONS

Please refer to the statewide policy glossary at http://www.state.nj.us/it/ps/glossary/index.html.

5 POLICY

The inclusion of security requirements during the design, development, implementation or managing information assets supporting business processes is essential to meeting security objectives.

System requirements for information security and processes for implementing security should be integrated in the early stages of information system projects. Controls introduced at the design stage are significantly less expensive to implement and maintain than those included during or after implementation.

All security requirements should be identified at the requirements phase of a project – prior to development and implementation. They should be justified, agreed upon, and documented as part of the overall business case for an information system.

Information security services and products are essential elements of the State's information security program, and are widely available and regularly used. Security products and services should be selected and used within the State's overall program to strengthen the State's information security infrastructure, and to protect the State's mission-critical assets. In the acquisition of both, departments/agencies should apply risk management principles to assist in the identification and mitigation of risks associated with the acquisition as described in 14-02-NJOIT, *115 – Information Security Risk Management Policy*.

When new products are acquired, a formal testing and acquisition process should be followed. Contracts with the supplier should specify security requirements. When the security controls built into in a proposed product do not satisfy the specified requirements, then the risk introduced and associated compensating controls must be considered prior to purchasing the product. When unneeded functionality is supplied and causes a security risk, this functionality must be disabled. When functionality is needed that causes a security risk, the risks and benefits must be reviewed, and, whenever possible, a compensating control structure must be put in place.

6 RESPONSIBILITIES

Each person involved in the acquisition and installation of information security products must understand the importance of keeping systems and data safe. Department and agencies are responsible for assigning the appropriate staff to the security roles required to meet the requirements of information security projects.

7 EXCEPTIONS AND NON-COMPLIANCE

Failure to comply with this policy may result in disciplinary action. Requests for exceptions for non-compliance with this policy shall be processed in accordance with Policy 08-02-NJOIT, *111 Information Security Managing Exceptions.*