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 141 – Security Awareness Program Policy	**POLICY NO:** 12-01-NJOIT	
	SUPERSEDES: NEW	**EFFECTIVE DATE:** 03/21/2012
	VERSION: 2.0	**LAST REVIEWED:** 01/21/2016

ATTN: Directors of Administration and Agency IT Managers

1 PURPOSE

The purpose of the Security Awareness Program Policy is to describe the requirements for ensuring that each employee receives adequate training about information security. Protecting the State of New Jersey's intellectual property, infrastructure, and any personal or confidential information is of utmost importance. Almost daily, reports of security breaches related to the theft or release of personal information are evident in the news. Firewalls, antivirus software, and upgrading computer software provide computer protection, but the first line of defense is employee awareness. An employee's knowledge of information security will help reduce the number of threats and help protect the State of New Jersey's infrastructure.

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 in its entirety applies to Executive Branch personnel.

4 POLICY

Departments and agencies will support and collaborate to institute a statewide information security awareness program. Working with HRDI, annual online training will be provided to employees, through the State's eLearning system.

In addition to the annual training, the State will provide additional reinforcement education such as newsletters, screen savers, webcasts, and other means through the State's NJInfosecure one-stop web site for computer and information security updates, alerts and advisories (http://www.cyber.nj.gov/).

5 REFERENCES

5.1 State of New Jersey

5.1.1 The State of New Jersey Identity Theft Act requires education and training of employees on the proper use of the computer security system and the importance of personal information security.

5.1.2 The State's Information Security Program is based on ISO 27002 (Information Security Management), which requires all employees of an organization to receive appropriate awareness training and regular updates.

5.2 Federal government

5.2.1 Health Insurance Portable and Accountability Act (HIPAA)

5.2.1.1 Requires the implementation of a security awareness and training program for all members of its workforce (including management).

5.2.2 Federal Information Security Management Act (FISMA)

5.2.2.1 Requires Federal agencies to provide security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of an agency, of information security risks associated with their activities and their responsibilities in complying with agency policies and procedures designed to reduce these risks.

5.3 Private Industry

5.3.1 Payment Card Industry (PCI) Data Security Standard (DSS)

5.3.1.1 Requires the State of New Jersey to protect and safeguard credit card holder information and to achieve compliance with the Payment Card Industry (PCI) Data Security Standard (DSS). PCI-DSS requires that all employees are made aware of the importance of cardholder information security through a security awareness program.

6 RESPONSIBILITIES

6.1 Administrative Directors working in conjunction with the Agency IT Director shall be responsible for ensuring the effective implementation of all statewide information technology circulars.

6.2 Departments and agencies working with OIT will provide a communication plan on how to notify employees of the State's online information security awareness training.

6.3 Departments and agencies will grant employees access to the State's online information security awareness training, and have employees take annual updates of the training as appropriate.

6.4 Departments and agencies will have Human Resources add the State's online information security awareness training to their new employee orientation package.

6.5 Departments and agencies will use the State's eLearning system to record employees' training, and the results maintained in personnel files as part of the employee's permanent record.

6.6 Departments and agencies will report to OIT when training is complete for all employees by sending an email to njinfosecure@oit.nj.gov.

7 EXCEPTIONS AND NONCOMPLIANCE

Departments and Agencies shall comply with this policy within 90 days of its effective date.

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 business reasons or system constraints. Exceptions and non-compliance with this

policy shall be managed in accordance with Policy 08-02-NJOIT, *111 – Information Security Managing Exceptions*.