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 142 – Workforce Security Policy	**POLICY NO:** 15-01-NJOIT	
	SUPERSEDES: NEW	**EFFECTIVE DATE:** 01/22/2015
	VERSION: 1.0	**LAST REVIEWED:** 01/22/2015

ATTN: Directors of Administration and Agency IT Managers

1 PURPOSE

The purpose of the Workforce Security Policy is to describe the requirements for employees in helping to protect the intellectual property, technological infrastructure and data security of the State of New Jersey's Executive Branch.

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

Each state agency shall:

4.1.1 In accordance with State and Federal laws and regulations, verify the identity and employment eligibility as well as conduct required background screenings of all State employees and contractors before granting them access to State facilities or information resources that are not designated as public

access resources. Reference the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12, *An Introduction to Computer Security: The NIST Handbook*, Section 10.1.3, *Filling the Position – Screening and Selecting*. Unfavorable results of background screening are not in themselves causes to refuse employment.

4.1.2 Ensure that only workforce personnel with the business need to access personal, confidential, proprietary, and/or sensitive information be granted access to such non-public resources.

4.1.3 Ensure that newly hired or transferred individuals (including employees of third-party service providers) meet established security and qualification criteria for their positions.

4.1.4 Work with the State's Human Resources Development Institute (HRDI) to ensure that newly hired personnel (including employees of third-party service providers) receive security awareness training within four weeks of hire as specified in 12-01-NJOIT, *141 – Security Awareness Program Policy.*

4.1.5 Define and explain security responsibilities for each system user's role and make clear the ramifications of failing to comply. Provide sufficient training and supporting reference materials that describe ways to protect state-owned information assets and resources. Authorized personnel shall review the department / agency's confidentiality and non-disclosure policy, and sign a non-disclosure agreement that details the rules of behavior.

4.1.6 Ensure that organizational information and information systems are protected during and after personnel actions such as terminations and/or transfers.

4.1.7 Employ formal sanctions for personnel who fail to comply with security policies and procedures.

5 RESPONSIBILITIES

5.1.1 Administrative Directors working in conjunction with the Agency IT Director shall be responsible for enacting the policies specified in 12-01-NJOIT, *141 – Security Awareness Program Policy.*

5.1.2 Departments and agencies shall be responsible for enacting these policies and the policies specified in 12-01-NJOIT, *141 – Security Awareness Program Policy.*

5.1.3 The supervisors and/or managers of a business entity's workforce are responsible for determining and authorizing each assigned workforce member's access to any information system that houses protected

information. A workforce member may not authorize his own access to an information system that houses protected information.

6 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*.