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 171 – Minimum System Security and Protection Policy	**POLICY NO:** 14-01-NJOIT	
	SUPERSEDES: NEW	**EFFECTIVE DATE:** 01/23/2014
	VERSION: 2.0	**LAST REVIEWED:** 01/23/2014

ATTN: Directors of Administration and Agency IT Leaders

1 PURPOSE

The purpose of this policy is to specify the minimum security requirements for infrastructure, computing devices, and computer systems supporting the Executive Branch of State Government. This policy establishes the guidelines for technical and non-technical security controls.

2 AUTHORITY

This policy is established under the authority of the State of New Jersey. N.J.S.A. 52:18a-230 b. This statute 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 all personnel including employees, temporary workers, volunteers, contractors and those employed by contracted entities, and others who are authorized to access to State's infrastructure devices, portable computing devices and computer systems.

4 DEFINITIONS

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

5 POLICY

It's authors intend this policy to set the parameters for a balanced information security program that addresses the management, operational, and technical aspects of protecting information and information systems.

Their intent is to create a repeatable approach for selecting and specifying security controls for infrastructure, computing devices, and computer systems so that the Executive Branch meets minimum security requirements.

6 RESPONSIBILITIES

6.1 Departments and Agencies

6.1.1 Information Technology Directors, Managers, and Supervisors shall ensure the minimum security requirements are applied to all infrastructure, computing devices, and computer systems under their control. IT Managers and Supervisors shall report compliance anomalies to their IT Director or designee.

6.1.2 All Departments and Agencies are required to adhere to *11-02-NJOIT, 190-NJOIT – Information Security Incident Management Policy* and to report security incidents according to the procedures outlined in *11-02-P1-NJOIT, 190-00-01 – Information Security Incident Management Reporting Procedures.*

6.2 State of New Jersey IT Administrators

6.2.1 All Administrators who prepare, administer, and maintain devices and computer systems shall ensure that the minimum security requirements are implemented on the infrastructure, computing devices, and computer systems 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.

6.2.2 All external providers of critical information system services, used by any agency, must also carry out all appropriate security control measures put in place by the agency. Agencies must explicitly contract these measures with their external service providers.

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