**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**<br><br>162 – System Planning and Acceptance Policy | **POLICY NO:** 14-06-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 System Planning and Acceptance policy is to provide for a continuous process that will minimize the risk that system failures pose to infrastructure, computing devices, and computer systems supporting the Executive Branch of State Government. System and data availability and data confidentiality and integrity are security concerns. Therefore, State IT personnel must engage in advance planning and preparation to ensure the availability of adequate capacity for and protection of State information. This policy establishes guidelines for technical and non-technical security controls that will be applied to new and upgraded State of New Jersey information systems, including both networks and applications.

# 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 during the planning and acceptance phases of the system lifecycle for every State infrastructure device, portable computing device and computer system. The principles described in this policy also apply to the planning and acceptance of systems provided for State use by organizations outside New Jersey.

# 4 DEFINITIONS

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

# 5 POLICY

Planning and preparation during the design of State information systems is essential to ensure the availability [XE "availability"] of adequate capacity and put security controls in place. This planning will require testing of new systems for stress, capacity, and peak loading. These systems must demonstrate a level of performance and resilience that meets or exceeds the technical and business needs and requirements of the State.

Accordingly, the State of New Jersey will establish the security protocols associated with the availability of adequate capacity and resources to deliver the required system performance, availability, and reliability. This capacity will be identified through advance planning and preparation that will include projections of future capacity requirements to reduce system overload and outage risks. In addition, operational requirements for new information systems will be established, documented, and tested prior to acceptance and use.

This policy also establishes a repeatable approach for selecting and specifying security controls for infrastructure, computing devices, and computer systems to meet the applicable technical and non-technical minimum-security requirements.

# 6 RESPONSIBILITIES

## 6.1 Departments and Agencies

6.1.1 Information Technology Directors, Managers, and Supervisors will ensure that Minimum-Security Requirements Standards are applied to all planned infrastructure, computing devices, and computer systems under their control. IT Managers and Supervisors shall report exceptions to the standards to their IT Director or designee.

6.1.2 All Departments and Agencies must adhere to the 190-NJOIT Incident Management Reporting policy and report security incidents according to the procedures outlined in 190-00-01 Information Security Incident Management Reporting procedure.

## 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 requirement

standards are implemented on the infrastructure, computing devices, and computer systems under their control.

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 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*.