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** 110 – Security Framework Policy	**POLICY NO:** 12-03-NJOIT	
	SUPERSEDES: NEW	**EFFECTIVE DATE:** 07/17/2012
	VERSION: 2.0	**LAST REVIEWED:** 01/21/2016

ATTN: Directors of Administration and Agency IT Managers

1 PURPOSE

A Security Framework is a comprehensive information security model that ensures the overall security of information by not only focusing on technological issues, but also addresses other principal elements of an organization such as people, processes, and business strategies, which can also mandate the need for information security. The purpose of this policy is to provide a Security Framework to create security safeguards, best practices, and standards. The policy also offers a dynamic security plan to protect the State of New Jersey's infrastructure and critical assets.

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 to all personnel, including employees, temporary workers, volunteers, contractors and those employed by contracted entities, and others who administer enterprise information resources.

4 POLICY

The Security Framework establishes the general, overarching guidance on matters affecting information security. This Framework establishes security standards and practices based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the International Standards Organization (ISO) 27002 Information Security Management System (ISMS).

The NIST Cybersecurity Framework guide cybersecurity activities and risk management processes. The NIST Cybersecurity Framework consists of three parts (http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf):

4.1.1 Core

4.1.2 Implementation Tiers

4.1.3 Profile

The Framework Core consists of four elements, 1) Functions, 2) Categories, 3) Subcategories, and 4) Informative References.

The Implementation Tiers provide context to cybersecurity risks within our organization.

The Profile identifies opportunities and improvements by comparing current to target organization's profiles (the state of cybersecurity.)

The ISO 27002 is a comprehensive set of controls comprised of the best practices in information security. The ISO 27002 standard consists of the following twelve main sections:

4.1.4 Security Policy

4.1.5 Risk Assessment

4.1.6 Organization of Information Security

4.1.7 Asset Management

4.1.8 Human Resources Security

4.1.9 Physical and Environmental Security

4.1.10 Communications and Operational Management

4.1.11 Access Control

4.1.12 Information Systems Acquisition, Development and Maintenance

4.1.13 Information Security Incident Management

4.1.14 Business Continuity Management

4.1.15 Compliance

The Statewide Office of Information Security references the following information security requirements as part of the Security Framework, which can be mapped back to the NIST Cybersecurity Framework and ISO 27002 Information Security Management System.

4.1.15.1 HIPAA Security – Health Insurance Portability and Accountability Act of 1996, 42 USC 1301 et seq., and the associated regulations at 45 CFR parts 160 and 164

4.1.15.2 IRS – Security Guidelines For Federal, State, And Local Agencies – Publication 1075

4.1.15.3 FISMA – Federal Information Security Management Act of 2002, Public Law 107-347. NIST Special Publication 800-53, Recommended Security Controls For Federal Information Systems

4.1.15.4 Payment Card Industry (PCI) Data Security Standard (DSS) and Payment Application Data Security Standard (PA-DSS)

4.1.15.5 State Of New Jersey Identity Theft Prevention Act, June 2005

4.1.15.6 State of New Jersey Drivers' Privacy Protection Act of 1994, pub.L.103-322

4.1.15.7 NIST (National Institute Of Standards and Technology) Publications

4.1.15.8 Information Technology standards and other applicable information security or confidentiality guidelines.

5 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 noncompliance with this policy shall be managed in accordance with Policy *08-02-NJOIT, 111 – Managing Exceptions.*