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 181 Encryption and Digital Signatures Policy	**POLICY NO:** 14-26-NJOIT	
	SUPERSEDES: NEW	**EFFECTIVE DATE:** 10/27/2014
	VERSION: 1.0	**LAST REVIEWED:** 10/27/2014

ATTN: Directors of Administration and Agency IT Managers.

1 PURPOSE

Certain federal and State laws require implementation of safeguards to protect the privacy and integrity of confidential, proprietary, and/or sensitive information that is transmitted or stored. The purpose of this policy is to implement safeguards to ensure that all electronic usage of confidential, proprietary, and/or sensitive information is protected from unauthorized access, disclosure, alteration, deletion, and/or transmission. In addition, the author of such information should be verifiable to very high level of certainty.

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 applies to all State of New Jersey's Departments, Agencies, their employees, contractors, consultants, temporary workers, and others who are authorized to access enterprise assets and information resources.

4 DEFINITIONS

Please refer to the Statewide Policy Glossary at http://www.state.nj.us/it/ps/glossary/index.html.

5 POLICY

State agencies shall apply appropriate encryption technologies (plural) to reduce the risk that unauthorized parties are able to access and use electronic information. Agencies shall employ appropriate encryption technologies (plural) to protect personal, confidential and/or sensitive information as defined in 08-04-S1-NJOIT, *130-01 Asset Classification and Control Standard*. Encryption technologies can also be a compensating control for other classifications of information when traditional physical or logical security cannot be applied.

Agencies shall conform to the following requirements:

5.1.1 For data with sensitivity level of confidential or higher (more restrictive), encryption requirements shall be enforced for data regardless of at rest or in transit, in accordance with FIPS 140-2 specifications.

5.1.2 Data at Rest

5.1.2.1 All State proprietary and/or data with a sensitivity level of confidential or higher, stored in databases or on removable storage or portable computing devices must be protected with appropriate encryption technologies.

5.1.2.2 Encryption must be used when storing passwords, financial, medical, and/or personal data.

5.1.2.3 All computing devices that store confidential, proprietary, and/or sensitive information must employ appropriate encryption technologies – including pre-boot authentication – to the greatest extent possible.

5.1.2.4 Devices using full disk encryption must not to be placed in suspend mode when unattended outside of the secured office location and are to be shut down completely when not in use or when unattended.

5.1.3 Data in Transit

5.1.3.1 All mobile computing devices capable of using wireless encryption for network communication must do so when connected wirelessly to a State network. Devices not capable of using wireless encryption are not

to be connected wirelessly to the State network or to any device attached to a State network.

5.1.3.2 All personnel shall use appropriate encryption technologies when connecting remotely to the Next Generation Services Network (NGSN) when accessing State data with a sensitivity level of confidential or higher.

5.1.3.3 Wireless access points are to be configured to use AES-256 encryption, at a minimum.

5.1.3.4 When an application requires authentication using a web application protocol, it must use cryptographic protocols such as Transport Layer Security (TLS) or Secure Socket Layer (SSL).

5.1.4 Digital Signature

5.1.4.1 Digital signatures must originate from the State's Enterprise Managed Public Key Infrastructure (MPKI).

5.1.4.2 PKI Certificates must adhere to the IETF (Internet Engineering Task Force) X.509 standard.

5.1.4.3 Public key certificates must be readily accessible to any entity that wishes to authenticate another entity.

5.1.4.4 Agencies may become a Sub-Certificate Authority through the State's Enterprise Certificate Authority.

5.1.4.5 A private key must remain accessible to its owner.

5.1.5 Key Management

5.1.5.1 Key management responsibility may only be delegated to an individual who has signed a confidentiality agreement.

5.1.5.2 Products to develop encryption keys as well as the keys themselves shall be kept secured when not in use and throughout the life cycle of the information.

5.1.5.3 Keys used for digital signatures, digital certificates, and user authentication shall not be included in a key escrow arrangement with a third party.

5.1.5.4 The crypto-period (the time a key can be used for signature verification or decryption) shall be determined based on the sensitivity of the information and the risk of key compromise.

6 ROLES AND RESPONSIBILITIES

6.1.1 An agency must be responsible to implement and enforce encryption and digital signature policies required by this document.

6.1.2 Authorized Users shall be responsible for complying with all State policies, standards, and guidelines referenced within this policy. In addition, authorized users shall comply with all applicable government codes of ethics and the New Jersey Conflicts of Interest Law.

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.*