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 173 -Wireless Network Security Policy	**POLICY NO:** 14-03-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

This policy defines how New Jersey's Executive Branch deploys, administers and supports wireless technologies within its computer, telecommunications and other electronic information networks. Its goal is to safeguard access points to these networks by establishing minimum requirements, rules and responsibilities needed to mitigate security risks introduced by wireless technologies.

This policy does not address cellular or other wireless technologies or services supplied by outside vendors or service providers such as remote users accessing the Next Generation Services Network (NGSN) from wireless networks outside of State control. OIT will cover requirements, rules and responsibilities for remote access in another policy.

2 AUTHORITY

This policy is established under the authority of the State of New Jersey N.J.S.A. 52:18a-230 b. This order defines New Jersey Office of Information Technology's (NJOIT) role in regards to information technology within the community of the Executive Branch of State Government.

The New Jersey Office of Information Technology reserves the right to change or amend this circular.

3 SCOPE

This policy applies to all State of New Jersey Departments, Agencies, "in but not of" entities (hereinafter referred to as "Agency"), their employees, contractors, consultants, temporary workers and others who develop and administer information

systems and resources for those systems. Any authority or other entity that regularly accesses State networks with wireless devices shall also follow the guidelines in this policy.

The policy's scope includes the following:

3.1.1 Information assets used by the Executive Branch of New Jersey State Government for external and client operations.

3.1.2 Physical assets that process store or transmit information for the Executive Branch of New Jersey State Government.

3.1.3 Wireless communication device(s) capable of transmitting packet data that are connected to any of the State's internal networks.

4 DEFINITIONS

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

5 POLICY

5.1.1 Users should access the State's wireless networks in a secure manner, following the current standards of the Institute of Electrical and Electronics Engineers (IEEE) for wireless access.

5.1.2 Each authorized user with access to the State's Wireless Local Area Networks (WLAN) must adhere to this policy and the corresponding referenced materials. Users should consult the referenced State policies cited in this document for additional guidance. Use of State-provided or configured computers or wireless communications devices constitutes consent to this policy and all related State policies.

5.1.3 All WLAN users shall only use products and security configurations approved by OIT. Agencies must follow the standard procedures for requesting wireless access.

5.1.4 This policy prohibits all synchronization with IT devices that are not approved/supported by OIT and the user's Agency. Only hardware and software consistent with State standards shall be used for wireless networking.

5.1.5 Should wireless policies or standards of the Agency conflict with those of OIT, the more stringent standards shall apply.

5.1.6 This policy does not apply to wireless devices and/or networks that are not or will not be connected to the Garden State Network, provided those wireless devices and/or networks do not interfere with the operations of the Garden State Network.

5.1.7 Wireless devices connected to networks other than the Garden State Network shall have the appropriate security controls installed before they are connected to the NGSN or other State networks. Reference 173-01 Wireless Network Security and 11-01-NJOIT 179 – Remote Access and the Extranet Policies, Standards and Procedures.

5.1.8 No user can connect a wireless device to an independent network and the Garden State Network at the same time. If needed, exceptions must be cleared by OIT. In general, no user should connect to both a wired network and a wireless LAN at the same time, if the device is or will be used to connect later to State networks.

5.1.9 If a guest network is required, the requesting Agency must contact the OIT Wide Area Network for requirements and information.

5.1.10 In the event that a wireless device interferes with other State equipment, the appropriate Network Administrator or designee shall resolve the interference problem. If the Network Administrator is unable to resolve the issue, it will be the responsibility of the Agency IT Leader, CTO or their designee to resolve the problem.

5.1.11 The NIST Guidelines for Securing Wireless Local Area Networks (WLANs) are the standard for this policy. Any solution, specification or requirement must meet the NIST Special Publication 800-153 Guidelines for Securing Wireless Local Area Networks (WLANs) document.

5.1.12 Agencies subject to the Payment Card Industry's Data Security Standard (PCI DSS) compliance should reference the PCI DSS Wireless Guidelines for guidance on installation, testing and/or deploying 802.11 Wireless Local Area Networks (WLAN).

5.1.13 OIT will review this policy annually and update as required to keep pace with technological advances.

6 RESPONSIBILITIES

Authorized Users shall be responsible for abiding by the State's policy regarding the use of wireless networking equipment, including acquiring any required written

authorization from OIT or their Agency before purchasing, attaching, using and/or activating any such equipment on any Agency computer.

6.1 Agency IT Leader shall be responsible for:

6.1.1 Implementing, managing and maintaining their local wireless access points. If multiple Agencies need a connection between Agencies, they must request approval from the OIT Wide Area Network (WAN) unit.

6.1.2 Requesting approval from OIT's Wide Area Network unit for installation of wireless technology that operates between different buildings on a campus.

6.1.3 Ensuring immediate removal of any wireless networking device, software and/or hardware on the local Agency's network that was installed without written permission. Additionally. IT leaders must report policy violations to the OIT Network Control Center (NCC), especially if they suspect that a device was installed for the purpose of compromising the local network.

6.1.4 Informing users of State wireless assets of the State's wireless communications policies.

6.1.5 Ensuring appropriate IT personnel are properly trained in the use of wireless communications technology. Network administrators shall be trained so that they are fully aware of the security risks posed by WLANs and wireless devices. They should work to ensure compliance with security policies and know what steps to take in the event of a cyber attack.

6.1.6 Resolving wireless communication interference problems at the Agency's network site. Monitoring performance and network statistics of all local wireless Agency networks. Maintaining security as required to prevent unauthorized access to the local network.

6.1.7 Ensuring that employees, temporary workers, volunteers, contractors and those employed by contracting entities cannot deploy unapproved or unregistered wireless communications systems or devices on State equipment or networks.

6.1.8 Maintaining information regarding wireless bridging between and among Agency networks and access points. All existing information on wireless bridges must be sent to OIT's WAN unit.

6.2 New Jersey Office of Information Technology (OIT)

The New Jersey Office of Information Technology shall be responsible for providing physical and technical safeguards for the electronic assets of the State. OIT, therefore, shall:

6.2.1 Monitor the enterprise level wireless networks and the handling/reporting security incidents, violations, etc., in accordance with established statewide policies.

6.2.2 Perform operations and monitoring to ensure confidentiality, authentication, integrity and non-repudiation of information systems and information as determined by this policy and related statewide policies.

6.2.3 Develop, maintain, and update wireless communications policies, security standards and procedures.

6.2.4 Maintain registration of all statewide wireless networks and access points.

6.2.5 Provide configuration, management and deployment of statewide wireless communications systems.

6.2.6 Approve statewide standards for wireless communication hardware and software used by Agencies.

6.2.7 Provide assistance for the development, management and deployment of statewide wireless communication networks.

6.2.8 Perform network scans to ensure that unapproved and unregistered wireless network devices are not operating on State of New Jersey networks.

6.2.9 Manage the development of wireless network technologies, evaluate technology enhancements and incorporate new wireless network technology within the State's network infrastructure.

7 EXCEPTIONS AND NON-COMPLIANCE

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 due to a business reason or system constraint. Exceptions and noncompliance with this policy shall be managed in accordance with Policy 08-02-NJOIT, *111 – Information Security Managing Exceptions.*