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 174 – Network Security Policy	**POLICY NO:** 14-18-NJOIT	
	SUPERSEDES: NEW	**EFFECTIVE DATE:** 06/12/2014
	VERSION: 1.0	**LAST REVIEWED:** 06/12/2014

ATTN: Directors of Administration and Agency IT Managers

1 PURPOSE

The purpose of this policy is to define the requirements for Network Security that protect the State of New Jersey's Next Generation Services Network (NGSN). The policy's goal is to minimize potential for unauthorized access to the NGSN, loss of sensitive or confidential information, and/or damage to the State of New Jersey's critical internal systems and information technology 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

This policy applies to all State of New Jersey Departments, Agencies, State Authorities, "in but not of" entities, their employees, contractors, consultants, temporary employees, and other workers including all personnel who are tasked with the protection of the State of New Jersey resources and the NGSN.

4 DEFINITIONS

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

5 POLICY

The following requirements provide a policy for delivering a secure NGSN:

5.1.1 A baseline network configuration shall be created for the NGSN. Changes to any NGSN device's hardware, software, or operating environment such as patches shall be tested, applied and documented in accordance with Change Management protocols.

5.1.2 Any wireless device or wireless computer system connected to the NGSN shall be configured to protect the information transmitted according to the sensitivity and criticality of that information, in accordance with 14-03-NJOIT, *173 – Wireless Network Policy*.

5.1.3 Any wireless device or wireless computer system connected to the NGSN shall be configured so that it does not reveal information about the device or system, or about the network architecture, except to identify the SSID or network by name.

5.1.4 Distribution of any IP addresses will be centrally managed by State of New Jersey Network WAN administrators who will be responsible for planning, tracking, and managing the IP space used in the network.

5.1.5 State of New Jersey network administrators have the responsibility to centrally manage Domain Name Services (DNS) names for the State's external and internal domains.

5.1.6 All servers in the NGSN shall be assessed for hardening requirements. The evaluation results will be reported.

5.1.7 All connections of the NGSN to external networks must be, at a minimum, under the protection of a firewall. Demilitarized Zone (DMZ) networks require firewalls to protect their hosts from direct outside attacks, and their connections to other internal networks must also have firewall protection.

5.1.8 Any device or computer system that is connected to the NGSN:

5.1.8.1 Shall use security controls for administrative access to any network device or computer system that is connected to the network in accordance with 14-01-NJOIT, 171 – Minimum System Security and Protection Policy. Administrative access from a public or uncontrolled network to the NGSN shall not be permitted unless such access is essential to business operations and has been approved through an exemption request, per 08-02-NJOIT, 111 Information Security Managing Exceptions. In all such cases, encryption shall be used for remote administrative connections.

5.1.8.2 Shall be configured so that it does not reveal information about the device or system, or about the NGSN architecture, except to the extent that such information is necessary to the operation of the network, device, or system.

5.1.8.3 Shall be configured, to the extent possible, to record information related to security events to a log.

5.1.8.4 Shall be configured to reduce the risk that the device or system will be compromised. Security patches and anti-virus software related to security shall be applied to a device or system in a timely manner in accordance with 14-09-NJOIT 168 – Change Management Policy and 12-04-NJOIT, 184- Information Security Vulnerability Management Policy.

5.1.8.5 Shall have its network cabling installed and/or maintained by only qualified personnel. Agencies shall implement safeguards to protect network cabling from being damaged and to reduce the possibility of unauthorized interception of data transmissions that take place across such cabling.

5.1.8.6 Shall be protected physically and logically from unauthorized access and use.

5.1.9 Non-emergency Maintenance on the NGSN will be scheduled, and all agencies will be notified within 5 days of the maintenance and informed of the duration and impact in accordance with 14-09-NJOIT, *168 – Change Management Policy*. Every effort should be made to schedule this type of maintenance during low use and low impact hours.

5.1.10 All agencies shall synchronize time on all network-attached devices at least once every 48 hours. A primary time server shall be assigned to which all devices are synchronized.

5.1.11 All Cyber Security incidences on the NGSN will be handled in accordance to 11-02-NJOIT, *190 NJOIT - Information Security Incident Management Policy.*

5.1.12 Personnel tasked with NGSN security responsibilities shall develop, document and implement security controls for the confidentiality, integrity, and availability of information processed, stored, or communicated on the NGSN.

5.1.13 All access control devices shall be limited to the least access necessary in order to meet the business requirements of the service, whenever technically possible.

5.1.14 Network monitors and audit controls should be used, especially in known risk areas, to check the network and traffic for unexpected (i.e. suspicious) content or behavior and other anomalies in order to protect state resources.

5.1.15 Vulnerability Assessments will be performed on all NGSN components in accordance with 12-04-NJOIT, *184 - Information Security Vulnerability Management Policy.*

5.1.16 Development and test environments will not be permitted to establish a connection with the NGSN unless authorized by NGSN administrators. Any ongoing access between these environments and the NGSN must be documented and presented to NGSN administrators for approval for continued use.

5.1.17 Agencies should ensure that backups of NGSN information are performed regularly and store these backup media in an offsite location, if possible. Disaster Recovery Plans and/or Contingency Plans should be in place documenting the recovery process in the event of a contingency situation.

6 ROLES AND RESPONSIBILITIES

6.1.1 The State of New Jersey

6.1.1.1 The NGSN Wide Area Network Unit within the Office of Information Technology will configure and manage the NGSN components in accordance with best practices and industry standards in order to protect the NGSN. Any Departments, Agencies, State Authorities, "in but not of " entities, requiring deviations from the standard configuration must formally request these changes and take responsibility for providing compensating controls to ensure the security of the NGSN.

6.1.1.2 To protect the NGSN, the Statewide Information Security Office within the Office of Information Technology will set up and manage the authentication of firewalls and perform the administrative functions needed to maintain the lifecycle management processes, in accordance with best practices and industry standards.

6.1.1.3 The Statewide Cyber Security Threat Mitigation committee will approve, publish, and update the security standards.

7 ENFORCEMENT

Any NGSN Authorized User found to have violated this policy may be subject to disciplinary action and loss of NGSN management privileges. In addition, violators may be subject to criminal prosecution, civil liability, or both for unlawful use of any access.

8 EXCEPTIONS AND NON-COMPLIANCE

Departments and Agencies shall comply with this policy within 90 days of its effective date.

Requests for exceptions for non-compliance with this policy shall be processed in accordance with Statewide IT Circular 08-02-NJOIT, *111 – Information Security Managing Exceptions*.