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 179-01 - Remote Access Standard	**POLICY NO:** **11-01-S1-NJOIT**	
	SUPERSEDES: NEW	**EFFECTIVE DATE:** 07/20/2011
	VERSION: 1.0	**LAST REVIEWED:** 07/20/2011

ATTN: Directors of Administration and Agency IT Directors

1 PURPOSE

The purpose of this document is to establish the standards for remotely connecting to the State of New Jersey's Garden State Network ("GSN"). The issuance of this standard is to minimize the potential exposure to the GSN from unauthorized access, 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 standard is established under the authority of State of New Jersey P.L.2007.c.56.

The New Jersey Office of Information Technology (NJOIT) reserves the right to change or amend this circular to comply with changes in NJOIT or other agency policies.

3 SCOPE

This standard applies to all State of New Jersey Departments, Agencies, their employees, contractors, consultants, temporary employees, and other workers including all personnel affiliated with third parties remotely utilizing access to the State of New Jersey information technology assets and the GSN.

4 RESPONSIBILITIES

Administrative Directors working in conjunction with the agency IT Directors shall be responsible for ensuring the effective implementation of statewide information technology circulars.

5 STANDARD

All State entities and all Authorized Users who will be participating in the utilization of Remote Access privileges must adhere to the standards outlined below:

5.1 Remote Access users will be authenticated by use of the State's multi factor authentication: 1) a unique User ID 2) a password and 3) an approved Authentication Security Device and a random security code.

5.2 Remote Access Authorized Users will be automatically disconnected from the State of New Jersey GSN after thirty minutes of inactivity. The Authorized User must then logon again to reconnect to the GSN. A single session will be limited to a maximum connection time of 24 hours. The Authorized User must then logon again to reconnect to the GSN.

5.3 Split tunneling is NOT permitted with Remote Access; only one network connection is allowed.

5.4 State owned devices: State of New Jersey employees must use approved devices, including personal computers when connecting to the State of New Jersey GSN via any approved Remote Access technology.

5.5 Non-State owned devices: By using Remote Access technology, Authorized Users must understand that their devices, when connected to the GSN become a de facto extension of the State of New Jersey's GSN. While connected to the GSN through Remote Access technology, all devices are subject to the same usage, security rules, and regulations that apply to the State of New Jersey's owned equipment, i.e., their devices must be configured to comply with this standard, and all other related State IT circulars and policy directives related to using the GSN. The State of New Jersey is not responsible for supporting or maintenance of a personal device.

5.6 Virtual Private Network (VPN) method: When actively connected to the GSN, Remote Access connections will force all traffic from and to the device over the Remote Access tunnel; all other traffic (i.e. Internet

connections) not destined for the GSN will be dropped. Internet use and access within the GSN will be controlled through the Authorizing Entity's Proxy and Internet Filtering system.

5.7 Minimum Security Standards

The minimum security standards for protecting a device including a computer is based on the potential security threats.

5.7.1 The software products should not be limited to just anti-virus software, but other solutions to prevent spyware or malware and intrusions.

5.7.2 Identify and locate the device and if necessary wipe the media remotely if lost or stolen.

5.7.3 Protect the device's media by encrypting the media.

5.7.4 The use of supported operating system, software and web browser with the ability to receive updates.

	Desktop	Laptops	Mobile Devices
Anti-virus	X	X	X
Anti-malware	X	X	
Firewall	X	X	
Intrusion Detection	X	X	
Remote wipe		X	X
Theft Locator		X	X
Encryption		X	X
Manufacturer supported			
- operating system	X	X	X
- software	X	X	X
- web browser	X	X	X

6 EXCEPTIONS AND NON-COMPLIANCE

Any exceptions to this standard will be reviewed by the Statewide Remote Access Subcommittee Group and require approval from the Statewide Office of Information Security.