NJ Office of Information Technology
Chris Christie, Governor
E. Steven Emanuel, Chief Technology Officer

P.O. Box 212
300 Riverview Plaza
Trenton, NJ 08625-0212

www.nj.gov/it/ps/

STATE OF NEW JERSEY IT CIRCULAR

Title: 179 – Remote Access Policy

NO: 11-01-NJOIT	**SUPERSEDES:** N/A
LAST REVIEWED: March 9, 2012	**DATE PUBLISHED:** March 9, 2012
VERSION: 1.0	**EFFECTIVE DATE:** Date of Signature
FOR INFORMATION CONTACT: Office of Policy and Planning	

ATTN: Directors of Administration and Agency IT Managers

I. PURPOSE

The purpose of this policy is to define the requirements for remotely connecting to the State of New Jersey's Garden State Network ("GSN"). The issuance of this policy 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.

II. AUTHORITY

This policy is established under the authority of State of New Jersey P.L.2007.c.56. That statute defines the Office of Information Technology's role with regard to technology within the Executive Branch of State Government.

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.

III. SCOPE

This policy 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 resources and the GSN.

IV. DEFINITIONS

A. Remote Access
Access that is provided using public communication links to connect remote users via client software to private network resources. This system uses encryption and other security mechanisms to ensure that only Authorized Users can access the GSN and that the data cannot be intercepted.

B. Authorizing Entity

For this policy, an Authorizing Entity is a State of New Jersey Department, Agency, State Authority, or an "in but not of" entity.

C. NJ Portal
An access method that provides Secure Socket Layer application connectivity to Private network hosts on the GSN via encrypted tunnels over the Public Internet.

D. Security Device
A network hardware device that enables secure connections to private network hosts via encrypted tunnels over the Public Internet.

E. Authorized User
State of New Jersey employees and third parties (customers, vendors, etc.) who are authorized by the Departments, Agencies, State Authorities and "in but not of" entities, who comply with the Remote Access policy and complete the appropriate Remote Access Registration Form(s).

F. User Managed Service
A service where the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, and installing any required software.

G. Split Tunneling
When connected via the Remote Access, it is a method that allows Internet destined traffic to be sent unencrypted directly to the Internet, which could compromise the GSN.

H. Authentication Security Devices
One-time, time synchronous password generators.

I. Accounting and Security Logs
Logs created from the Security Device and associated security access applications that detail the activity performed by a Remote Access Authorized User.

J. Event
Any Remote Access violation and/or suspicious activity that causes intentional and/or unintentional damage to or misuse of the State's information technology assets.

K. External Entities
Any person not defined as a State Employee.

L. Multifactor Authentication
Authentication based on proving identity by means of:

1. User id – "*unique identifier*" assigned to the Authorized User

2. Password – what the Authorized User "*know*"

3. Physical Token and random security code – what the Authorized User "*has*"

M. State Employee
State employees must be entered into the State's Personnel Management Information System (PMIS) or its successor.

N. Site Representative (**S**ite **V**irtual Private Network **R**epresentative - **SVR**)
The agency's coordinator will be responsible to track all agency requests for Remote Access, and act as the liaison between the users/vendors and NJOIT.

O. Local Registration Authority (LRA)
An agent for the agency's SVR, for vetting identities and gathering completed forms.

V. POLICY

The following requirements must be implemented by all State entities and all Authorized Users who remotely connect to the State of New Jersey's GSN:

A. All Authorized Users with a business need to utilize Remote Access must adhere to this policy and all related standard and procedure documents.

B. State of New Jersey employees and external entities (customers, vendors, etc.) who are authorized by the Departments, Agencies, State Authorities and "in but not of" entities may utilize the benefits of Remote Access.

C. Authorized Users of the Remote Access service are responsible for all charges associated with the Authorized User's location or workstation.

D. Remote Access use is only permitted for legitimate State business purposes.

E. Virtual Private Network (VPN) method: State of New Jersey employees must utilize state issued equipment meeting the State's minimum security standards when accessing the GSN through this method.

F. External entities can only use the State of New Jersey's Virtual Private Network (VPN) method for accessing the GSN.

G. GOTOMYPC method: State issued or Non-State equipment must meet the State's minimum security standards or more stringent secure controls when accessing a computer on the GSN through this method. The GOTOMYPC method is only available to State of New Jersey employees.

H. VPN and Citrix method: State issued or Non-State equipment must meet the State's minimum security standards or more stringent secure controls when accessing a server on the GSN through this method.

I. The Authorizing Entity is responsible for ensuring that unauthorized users are not allowed remote access or privileges to the State of New Jersey's information technology assets and/or GSN.

J. All remote access users must authenticate using the State's "multifactor authentication" method.

K. The Statewide Remote Access Subcommittee must approve all Remote Access solutions.

L. Authorized users must provide Remote Access registration information to their Authorizing Entity and SVR or LRA.

VI. ROLES AND RESPONSIBILITIES

A. The State of New Jersey

1. The Statewide Remote Access Subcommittee is responsible for maintaining and reviewing any changes to the Remote Access architecture and policies.

2. Authorizing Entities are responsible for enforcing appropriate security software and policies, distribution, tracking, and retrieval of authentication security devices, performing periodic reviews and audits of security, and providing their users with operational support. Each Authorizing Entity must collect and maintain Remote Access registration information of their Authorized Users.

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

4. The Statewide Information Security Office within the Office of Information Technology will set up and manage the authentication security devices and perform the administrative functions to maintain the lifecycle management processes, in accordance with best practices and industry standards in order to protect the GSN.

5. The Statewide Security Threat Coordination committee will approve, publish, and update the security standards.

B. Users

1. Remote Access Authorized Users must comply with this policy by ensuring that the security software and patch management software on their remote computers are installed, running, up-to-date, and active.

2. Authorized Users with Remote Access privileges are responsible for ensuring that unauthorized users are not allowed access to the State of New Jersey's information technology assets. User Identification (User Ids) and passwords are the confidential information of the State and, therefore, no User Ids or passwords are to be shared.

3. The Remote Access Authorized User must preserve the security of their Remote Access authentication mechanisms, security devices and any associated passwords.

4. The Remote Access Authorized User must promptly notify the Authorizing Entity of any changes in their Registration Form information, e.g., changes in name, e-mail address, employer information, or contact information.

5. The Remote Access Authorized User must promptly notify the Authorizing Entity if the security of their workstation, authentication security mechanism, device, or password is compromised.

VII. FORMS

Remote Access Registration Form(s)

- Appendix A - Non-State Employee Registration Form (PDF 88K)

- Appendix B - State Employee Registration Form (PDF 86K)

VI. ENFORCEMENT

Any Remote Access Authorized User found to have violated this policy may be subject to disciplinary action and loss of Remote Access privileges. IN ADDITION, VIOLATORS MAY BE SUBJECT TO CRIMINAL PROSECUTION, CIVIL LIABILITY, OR BOTH FOR UNLAWFUL USE OF ANY ACCESS.

VII. EXCEPTIONS AND NON-COMPLIANCE

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

I, _____, have read and understand the information in the Remote Access Policy and Standard. I will comply with the processes as stated. I have received copies of these documents.

Signature_____ Date: _____

NOTE: SVR and /or LRA – Please make a photocopy of this page and staple it to the State or NON-State employee Registration Form.

Thank you, Statewide Site VPN Representative (SSVR).

Signature on File *3/9/2012*

E. STEVEN EMANUEL **DATE**
Chief Technology Officer-NJ Office of Information Technology
State Chief Information Officer