



<p>State of New Jersey IT Circular</p> <p>Title: Remote Access Virtual Private Network (VPN)</p>	NO: 07-13-NJOIT	SUPERCEDES: 04-02-OIT
	DATE PUBLISHED: 05-03-2007	
	VERSION: 1.0	EFFECTIVE DATE: 05-03-2007
	FOR INFORMATION CONTACT: Office of Policy and Planning oitpolicy@oit.state.nj.us	

ATTN: Directors of Administration and Agency IT Managers

I. PURPOSE

The purpose of this document is to establish and define a policy, which will provide guidelines for the utilization of the Remote Access Virtual Private Network (VPN) connections to the State of New Jersey Garden State Network (GSN).

II. AUTHORITY

This policy is established under the authority of State of New Jersey P.L.2007.c.56.

III. 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 affiliated with third parties utilizing the Remote Access VPN to access the State of New Jersey computing resources and the GSN. The enterprise Remote Access VPN solution is only to be used for specific connections where security needs are high and where the NJ Portal cannot meet those high security needs. This policy applies to implementations of Remote Access VPN that are directed through a VPN Concentrator. Any exceptions to this policy will require approval from the Statewide Remote Access Subcommittee. The Statewide Remote Access Subcommittee Group was charged to research and implement secure remote access solutions for the GSN by the Statewide Network Planning Committee. The Group is comprised of members from State Departments, Agencies, State Authorities, and "in but not of" entities.

IV. DEFINITIONS

A. Remote Access VPN

A network that is constructed by 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 network 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. VPN Concentrator

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 VPN policy and who complete the appropriate VPN 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 VPN, it is a method that allows Internet destined traffic to be sent unencrypted directly to the Internet, which could compromise the network.

H. Authentication Security Devices

One-time, time synchronous password generators.

I. Accounting and Security Logs

Logs that are created from the VPN Concentrator and associated security access applications that detail the activity performed by a Remote Access VPN Authorized User.

J. Event

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

K. Digital Certificate

A Digital Certificate is a file that is stored on your computer, smartcard or USB key fob that identifies who you are. VPN client software may be configured to use this file to identify you, when initiating VPN services.

V. POLICY

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 may utilize the benefits of Remote Access VPNs, which are a User Managed Service. Authorized Users of the Remote Access VPN service are responsible for all charges associated with the Authorized User's location or workstation - such as an employee's home PC. All State entities and all Authorized Users that want to participate in the utilization of the Remote Access VPN must adhere to this policy and the standards outlined below:

- A.** Remote Access VPN use is permitted only for legitimate State business purposes.
- B.** It is the responsibility of individuals with Remote Access VPN privileges to ensure that unauthorized users are not allowed access to the State of New Jersey's internal networks. User Identification (User IDs) and passwords are the confidential information of the State and, therefore, no User IDs or passwords are to be shared. Digital Certificates are the property of the State of New Jersey, and are not to be shared or transferred.
- C.** Remote Access VPN users shall be authenticated in one of two ways: Either (1) a unique User ID and one-time password, or (2) a State-issued digital certificate, unique user ID and conventional password. All digital certificates shall comply with the State's policy for Public Key Infrastructure (PKI). It is expected that State employees will normally be issued Authentication Security Devices for one-time passwords while non-State personnel will normally be issued digital certificates.

- D.** When actively connected to the GSN, Remote Access VPNs will force all traffic to and from the PC over the Remote Access VPN tunnel; all other traffic (i.e. Internet connections) not destined for the GSN will be dropped.
- E.** Split tunneling is NOT permitted; only one network connection is allowed.
- F.** All computers, including personal computers, connected to the State of New Jersey internal networks via Remote Access VPN or any other technology must use up-to-date anti-virus software, including all current virus definitions.
- G.** Remote Access VPN 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 network. 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 network.
- H.** The Statewide Remote Access Subcommittee must approve the Remote Access VPN client software. The subcommittee will evaluate the proposed software during their monthly meeting. If warranted, further review and testing may be performed to determine the viability of the software on the GSN.
- I.** By using Remote Access VPN technology with personal equipment, Authorized Users must understand that their machines, when connected to the GSN become, from an information technology operating condition, a de facto extension of the State of New Jersey's GSN, and while in that connected operating mode using the GSN through Remote Access VPN technology, those machines are subject to the same usage and security rules and regulations that apply to the State of New Jersey's owned equipment, i.e., their machines must be configured to comply with this policy and all other related Treasury circulars and policy directives related to using the GSN.
- J.** Each Authorizing Entity must collect and maintain registration information, including, where applicable, digital certificate registration information in order to provide Remote Access VPN to Authorized Users. Some of this information may be considered personal information. Use of the Remote Access VPN is voluntary. The State of New Jersey does not plan on divulging information collected or information disclosed voluntarily, however, it may be required to do so, pursuant to a request under the Open Public Records Act, the Right to Know Law, or other State or Federal law pursuant to court order. More specific details regarding the State of New Jersey's Privacy Policy may be found at <http://www.nj.gov/nj/privacy.html>.

VI. ENFORCEMENT

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

VII. PROCEDURES

- A.** All Remote Access VPN Authorized Users and their supervisor must sign a VPN Registration Form that states they are aware of and agree to the Remote Access VPN Policy (see section VIII). The authorizing entity's CIO (or equivalent) must grant their approval on the registration form. Each Authorizing Entity granting a Remote Access VPN connection to the GSN must ensure that the Registration Form for each Authorized User is completed, executed and maintained on file at the Authorizing Entity's site.
- B.** Authorizing Entities must develop and implement distribution, tracking and retrieval procedures for Authentication Security Devices and, where applicable, digital certificates. Authorizing Entities must support Third Parties including vendors by maintaining the Authentication Security Devices and only providing passwords when necessary based on duration and need.
- C.** Periodic reviews and/or audits of security requirements must be made by the Authorizing Entity to ensure the integrity of the network.
- D.** OIT will maintain Accounting and Security Logs for at least a minimum of (30) thirty days. Only the Site VPN Representatives can make requests for utilization reports. The Accounting and Security Logs will only establish the time and date that a user has accessed the network, the IP address, which they came in on from the Internet, and the address they were assigned once they were in the Garden State Network. The Authorizing Entity must rely on logs from their firewalls and servers to monitor the user's access and actions while within their network.
- E.** The Authorizing Entity must report immediately any violations and incidents to the OIT Help Desk, so that appropriate actions (i.e. removal of access privileges and retention of logs) are taken to ensure the integrity of the network. The OIT Help Desk can be reached by calling 1-800-NCC-HELP or (609) 530-6200.

VIII. 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 VPN architecture and policies.
2. Authorizing Entities are responsible for enforcing appropriate anti-virus software, distribution, tracking and retrieval of authentication security devices, including the issuance and use of digital certificates, performing periodic reviews and audits of security and providing their users with operational support.
3. The Garden State Network Planning Wide Area Network Unit within the Office of Information Technology will configure and manage the VPN Concentrator in accordance with best practices and industry standards in order to protect the GSN. Any agencies 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 in order to maintain the lifecycle management processes, in accordance with best practices and industry standards in order to protect the GSN.

B. Users

1. Remote Access VPN Authorized Users must comply with this policy by ensuring that the anti-virus software on their remote computers and PCs is installed, up-to-date and active.
2. It is the responsibility of the Remote Access VPN Authorized User to preserve the security of their Remote Access VPN authentication mechanisms, security devices and any associated passwords.
3. It is the responsibility of the Remote Access VPN Authorized User to ensure that unauthorized users are not allowed access to GSN internal systems.
4. The Remote Access VPN Authorized User must promptly notify the Authorizing Entity of any changes in their VPN Registration Form information, e.g., changes in name, e-mail address, employer information, or contact information.
5. The Remote Access VPN Authorized User must promptly notify the Authorizing Entity if the security of their workstation, VPN authentication security mechanism, device or password is compromised.

IX. FORMS

VPN Registration Form(s)

- [Non-State Employee Registration Form](#) (PDF 88K)
- [State Employee Registration Form](#) (PDF 86K)

Signature on File

ADEL EBEID
Chief Technology Officer,
Office of Information Technology

05/03/2007

DATE