



State Capitol P.O. Box 2062
Albany, NY 12220-0062
www.its.ny.gov

New York State Information Technology Standard	No: NYS-S14-010
IT Standard:	Updated: 05/15/2015
Remote Access	Issued By: NYS ITS Standard Owner: Enterprise Information Security Office

1.0 Purpose and Benefits of the Standard

The purpose of this standard is to establish authorized methods for remotely accessing State resources and services securely.

Major security concerns with remote access include the lack of physical security controls, the use of unsecured networks, the connection of infected devices to internal networks, the availability of internal resources to external hosts, potential damage to State resources, and unauthorized access to State information. This standard attempts to address these concerns.

2.0 Enterprise IT Policy/Standard Statement

Section 2 of Executive Order No. 117 provides the State Chief Information Officer, who also serves as director of the Office of Information Technology Services (ITS), the authority to oversee, direct and coordinate the establishment of information technology policies, protocols and standards for State government, including hardware, software, security and business re-engineering. Details regarding this authority can be found in NYS ITS Policy NYS-P08-002, Authority to Establish State Enterprise Information Technology (IT) Policy, Standards and Guidelines.

Except for terms defined in this standard, all terms shall have the meanings found in <http://www.its.ny.gov/glossary>.

3.0 Scope

This standard applies to all New York State Entities (SE) and all NYS systems.

4.0 Information Statement

NYS allows for remote access when there is a clear, documented business need. Access may be allowed from State-issued or personally-owned devices, at the discretion of the SE and in accordance with the standards below. Such access must be limited to only those systems necessary for needed functions.

4.1. **Approved Methods of Remote Access** - approved methods of remote access to NYS systems are listed in order of preference.

- a. **Portals** - a server that offers access to one or more applications through a single centralized interface that provides authentication (e.g., web based portal, virtual desktop interface (VDI)).
- b. **Direct Application Access** – accessing an application directly with the application providing its own security (e.g., webmail, https).
- c. **Remote System Control** – controlling a system remotely from a location other than the State’s internal network.
- d. **Tunneling** - a secure communication channel through which information can be transmitted between networks (e.g., Virtual Private Network (VPN)).

4.2. **Required Controls**

- a. Any method of remote access must use a centrally managed authentication system for administration and user access.
- b. Devices and software used for remote access must be approved by the SE after review by the SE’s Information Security Officer/designated security representative. SE’s may provide blanket approvals based on this review.
- c. The authentication token used for remote access must conform to the requirements of the appropriate assurance level as per the [Identity Assurance Policy](#).
- d. Remote access sessions must require re-authentication after 30 minutes of inactivity.
- e. Remote access sessions must not last any longer than 24 hours.
- f. The SE must monitor for unauthorized remote connections and other anomalous activity and take appropriate incident response action as per the [Incident Response Standard](#).
- g. Tunneling specific controls:
 - (a) No split tunneling is allowed.
 - (b) Network controls regulating access to the remote access endpoint and between remote devices and SE networks are required.
 - (c) When a remote access device will have access to other networked devices on the State’s internal network, the remote device must be authenticated such that configuration of the device is compliant with applicable policies.

5.0 Compliance

This standard shall take effect upon publication. The Policy Unit shall review the standard at least once every year to ensure relevancy. The Office may also assess agency compliance with this standard. To accomplish this assessment, ITS may issue, from time to time, requests for information to covered agencies, which will be used to develop any reporting requirements as may be requested by the NYS Chief Information Officer, the Executive Chamber or Legislative entities.

If compliance with this standard is not feasible or technically possible, or if deviation from this standard is necessary to support a business function, SEs shall request an exception through the Enterprise Information Security Office [exception process](#).

6.0 Definitions of Key Terms

Remote Access The ability to access non-public computing resources from locations other than the State's internal network.

7.0 ITS Contact Information

Submit all inquiries and requests for future enhancements to the standard owner at:

Standard Owner
Attention: Enterprise Information Security Office
New York State Office of Information Technology Services
1220 Washington Avenue – Bldg. 7A, 4th Floor
Albany, NY 12242
Telephone: (518) 242-5200
Facsimile: (518) 322-4976

Questions may also be directed to your ITS Customer Relations Manager at:
Customer.Relations@its.ny.gov

The State of New York Enterprise IT Policies may be found at the following website:
<http://www.its.ny.gov/tables/technologypolicyindex.htm>

8.0 Review Schedule and Revision History

Date	Description of Change	Reviewer
04/18/2014	Original Standard Release	Thomas Smith, Chief Information Security Officer
05/15/2015	Removed references to state workforce	Deborah A. Snyder, Deputy Chief Information Security Officer
04/18/2016	Scheduled Standard Review	

9.0 Related Documents

- [National Institute of Standards and Technology \(NIST\) Special Publication 800-46, Guide to Enterprise Telework and Remote Access Security](#)
- [NIST Special Publication 800-113, Guide to SSL VPNs](#)
- [NIST Special Publication 800-114, User's Guide to Securing External Devices for Telework and Remote Access](#)