NEW YORK STATE OF OPPORTUNITY. Office of Information Technology Services

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: **Remote Access**	**Updated:** 4/13/2023
	Issued By: NYS Office of Information Technology Services **Owner:** Chief Information Security Office

1.0 Purpose and Benefits

This Standard establishes authorized methods for remotely accessing New York State (NYS) 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 Authority

Section 103(10) of the State Technology Law provides the Office of Information Technology Services (ITS) with the authority to establish statewide technology policies, including technology and security standards. Section 2 of Executive *Order No. 117*[1], established January 2002, provides the State Chief Information Officer with 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

[1] All references to Executive Order 117 refer to that which was originally issued by Governor George E. Pataki on January 28, 2002 and continued by Executive Order 5 issued by Governor Eliot Spitzer on January 1, 2007, Executive Order 9 issued by Governor David A. Patterson on June 18, 2008, Executive Order 2 issued by Governor Andrew M. Cuomo on January 1, 2011 and Executive Order 6 issued by Governor Kathy Hochul on October 8, 2021.

Policy, *NYS-P08-002 Authority to Establish Enterprise Information Technology (IT) Policies, Standards and Guidelines*.

3.0 Scope

This standard applies to all “State Entities” (SE), defined as “State Government” entities as defined in Executive Order 117, established January 2002, or “State Agencies” as defined in Section 101 of the State Technology Law. This includes employees and all third parties (such as local governments, consultants, vendors, and contractors) that use or access any IT resource for which the SE or ITS has administrative responsibility, including systems managed or hosted by third parties on behalf of the SE or ITS. While an SE may adopt a different policy/standard, it must include the requirements set forth in this one. Where a conflict exists between this policy/standard and a SE’s policy/standard, the more restrictive requirement will take precedence.

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 State Entities (SEs) and in accordance with the standards below. Such access must be limited to only those systems necessary for needed functions and be in compliance with SE’s telecommuting policies and any applicable federal or state compliance requirements.

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 (ISO)/designated security representative. SEs 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 NYS-P20-001 Digital Identity Policy and NYS-S14-006 Authentication Tokens Standard.

d. Remote access sessions must require re-authentication after 15 minutes of inactivity as per NYS-S14-013 Account Management Access Control Standard

e. Remote access sessions must not last any longer than 18 hours as per NYS-S14-013 Account Management Access Control Standard

f. The SE must monitor for unauthorized remote connections and other anomalous activity and take appropriate incident response action as per the NYS-S13-005 Cyber 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. Compliance is expected with all enterprise policies and standards. ITS may amend its policies and standards at any time; compliance with amended policies and standards is expected.

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

6.0 Definitions of Key Terms

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

7.0 Contact Information

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

Chief Information Security Office
Reference: NYS-S14-010
NYS Office of Information Technology Services
1220 Washington Avenue, Building 5
Albany, NY 12226
Telephone: (518) 242-5200
Email: CISO@its.ny.gov

Statewide technology policies, standards, and guidelines may be found at the following website https://its.ny.gov/policies

8.0 Revision History

This policy should be reviewed consistent with the requirements set forth in NYS-P09- 003 Process for Establishing Information Technology Polices, Standards and Guidelines.

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
02/24/2017	Update to Scope, contact information and rebranding	Deborah A. Snyder, Deputy Chief Information Security Officer
07/16/2020	Update to Authority, Scope and Contact Information	Karen Sorady, Acting Chief Information Security Officer
05/20/2021	Updated Scope language	Karen Sorady, Acting Chief Information Security Officer
4/13/2023	Updated Scope Language, revisions, and alignment with other policies and standards	Chris DeSain, Chief Information Security Officer

9.0 Related Documents

National Institute of Standards and Technology (NIST) Special Publication 800-46, Rev. 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security

NIST Special Publication 800-113, Guide to SSL VPNs

NIST Special Publication 800-114, Rev.1, User's Guide to Telework and Bring Your Own Device (BYOD) Security

NYS-P20-001 Digital Identity Policy

NYS-S13-005 Cyber Incident Response Standard

NYS-S14-006 Authentication Tokens Standard

NYS-S14-013 Account Management Access Control Standard

Working Remotely | New York State Office of Information Technology Services (ny.gov)