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 Policy	**No:** NYS-P23-001
IT Policy: **International Access to NYS Systems or Data**	**Issued:** 12/19/2023 **Issued By:** NYS Office of Information Technology Services **Owner:** Chief Information Security Office

1.0 Purpose and Benefits

The purpose of this policy is to establish the requirement for a case-by-case review of all requests to conduct NYS business activities from international locations that require access to non-public NYS systems or data.

A State Entity (SE) must review its business needs and technical requirements prior to approving access to non-public NYS systems and data from international locations in each instance due to the unique laws, regulations, and varying levels of risk in any given international location. This policy benefits SEs by ensuring that they have appropriately reviewed an individual request for international access and put appropriate safeguards in place to limit the risk of this access.

Failure to perform a review and implement appropriate safeguards could have a significant detrimental impact on non-public NYS systems or data beyond the scope of the individual SE.

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], issued January 2002, provides the State Chief Information Officer with the authority to

[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.

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 Enterprise Information Technology (IT) Policies, Standards and Guidelines*.

3.0 Scope

This policy applies to all "State Entities" (SE), defined as "State Government" in Executive Order 117, 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, it must include the requirements set forth in this one. Where a conflict exists between this policy and a SE's policy, the more restrictive policy will take precedence.

4.0 Information Statement

SEs must carefully consider the risks associated with conducting NYS business activities from an international location, and all access to non-public NYS systems or data from international locations must be authorized and documented by SE management. Various aspects of accessing non-public NYS systems and data from international locations have information security, legal, and privacy implications.

4.1 SE-owned information may be at heightened risk of being compromised when accessed from international locations. Per the NYS-P03-002 Information Security Policy, Section 4.4, Information Risk Management, risk assessments must include additional considerations when systems, services, or information will reside, or be accessed from, outside of the Contiguous United States (CONUS)[2] to ensure compliance with relevant statutory, regulatory, and contractual requirements. Risk assessment results, and the decisions made based on these results, must be documented.

Individuals who travel to international locations with the intent of accessing non-public NYS systems and data should consult with their SE's legal counsel to determine relevant laws and restrictions specific to destination locations. SEs have the responsibility to educate their staff on the requirements for secure handling of information, as well as developing and maintaining specific SE processes and procedures to mitigate any associated risks. SEs may wish to review the U.S. Department of State's Travel Advisories page for additional information: https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html/.

[2] SEs should consider any applicable compliance regimes when accessing certain data. For example, certain Federal agencies prohibit accessing their data outside of the legal jurisdictional boundaries of the United States; however, U.S. territories, military installations, and embassies are considered within the legal jurisdictional boundaries of the United States.

Information security considerations include, but are not limited to:

- International locations may monitor all network communications and data traffic;
- Potential for review and possible duplication of hard drives at entry/exit or other checkpoints;
- Absence of security controls on publicly available networks;
- Loss or theft of devices;
- Device tampering;
- Installation or download of software not authorized by the SE;
- Potential for remote monitoring via integrated camera and/or microphone; and
- Additional technical considerations will vary depending on the country where the individual is located.

Legal and privacy considerations include, but are not limited to:

- Certain Federal regulations prohibit regulated data from being stored in, or accessed from, international locations;
- The use of Virtual Private Networks (VPNs) and encryption technologies may not be legal in international locations;
- Some online behaviors that are legal in the U.S. are not legal in international locations (e.g., restrictions on social media activity, prohibited websites, etc.);
- International locations may have differing import and export controls;
- Privacy laws vary considerably and may be different than in the U.S.; and
- Foreign customs agents may require access to an electronic device or data, and may seize the device if the individual does not comply.

The considerations listed above are representative only and should not be viewed as encompassing all possible risks of accessing non-public NYS systems or data from international locations. These considerations, and any other factors deemed appropriate, must be reviewed, and instructions must be created and established by the specific SE's legal counsel, ISO/designated security representative, Information Technology department, or other stakeholders as designated by the SE, that outline the approval process and the required security controls to limit the risk of this access.

For SEs receiving services from the Office of Information Technology Services (ITS), explicit approval for international access must be obtained from the Chief Information Security Officer (CISO) and Chief Technology Officer (CTO). SEs who do not receive

services from ITS can reference Appendix A for security controls to better secure non-public NYS systems and data for access from international locations.

5.0 Compliance

This policy shall take effect upon publication. Compliance is required with all enterprise policies and standards. ITS may amend its policies and standards at any time; compliance with amended policies and standards is required.

If compliance with this policy is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, State Entities 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-P23-001
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: Policies | Office of Information Technology Services (ny.gov)

8.0 Revision History

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

Date	Description of Change	Reviewer
12/19/2023	Original Policy Release	CISO

9.0 Related Documents

Appendix A

Appendix A

Security controls that can reduce the risk of international access include, but are not limited to:

- Traveling with the minimum amount of State equipment required.
- All remote connections must be made through managed points-of-entry reviewed by the Information Security Officer (ISO)/designated security representative. See NYS-S14-010 Remote Access Standard.
- Additional security controls which assure the appropriate protection of SE systems or data in remote environments must be shared with an employee or third-party (individual) prior to them being granted remote access.
- Any devices accessing NYS systems or data taken internationally must have a hardened configuration developed for the express purpose of international travel, must not contain State information, and must not be capable of use on internal State networks. (e.g., loaner equipment that will not be joined to the Domain). This configuration must disallow the use of removable media obtained from any source.
- All devices must be encrypted in accordance with the statewide Encryption Standard.
- All devices must be fully patched and include endpoint security (e.g., antivirus, endpoint detection and response), and must be remotely manageable by mobile device management (MDM).
- All devices must have a local firewall policy that restricts inbound and outbound traffic as much as practicable.
- All network connections must be made using a State-issued cell phone or mobile hotspot configured with international data access. Do not use other public or private wireless networks.
- All devices must remain in personal possession while in public spaces and stored in a secure location such as a hotel safe when not in use.
- All devices must be powered off when not in use.
- Changing of all passwords to be used prior to traveling abroad and upon return.
- Fully wipe/reimage any device upon return.
- Remove access to work email from personal devices.
- Familiarization with local laws regarding online behavior.