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-P14-001
IT Policy: **Acceptable Use of Information Technology Resources**	**Updated:** 01/05/2023 **Issued By:** NYS Office of Information Technology Services **Owner:** Chief Information Security Office

1.0 Purpose and Benefits

Appropriate organizational use of information and information technology ("IT") resources, and effective security of those resources, require the participation and support of the individuals using or accessing such resources. Inappropriate use exposes the State to potential risks including, but not limited to, virus attacks, compromised network systems and services, and legal issues.

2.0 Authority

Section 103(10) of the State Technology Law provides the NYS 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 oversee, direct and coordinate the establishment of IT policies, protocols and standards for State government, including hardware, software, security and business re-engineering. Details regarding this authority can be found in ITS Policy, *NYS-P08-002 Authority to Establish State Enterprise Information Technology (IT) Policy, Standards and Guidelines*.

[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.

3.0 Scope

This policy applies to all "State Entities" ("SE"), defined as "State Government" entities as defined in *Executive Order 117*[2], issued January 2002, or "State Agencies" as defined in *Section 101 of the State Technology Law*. This includes employees and all other third parties (such as local governments, consultants, vendors, and contractors), that use or access any IT resource for which ITS has administrative responsibility, including systems managed or hosted by third parties on behalf of the ITS. While an SE may adopt a different standard, 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.This policy applies to users of any system's information or physical infrastructure regardless of its form or format, created or used to support SEs. It is the user's responsibility to read and understand this policy and to conduct their activities in accordance with its terms. In addition, users must read and understand NYS-P03-002 Information Security Policy, its associated policies, standards, and guidelines, and NYS-P11-001 Use of Social Media Technology Policy.

4.0 Information Statement

Except for any privilege or confidentiality recognized by law, users have no legitimate expectation of privacy during any use of the State's IT resources or in any data on those resources. Any use may be monitored, intercepted, recorded, read, copied, accessed, or captured in any manner including in real time, and used or disclosed in any manner, by authorized personnel without additional prior notice to users. Periodic monitoring may be conducted of systems used, including but not limited to all computer files and all forms of electronic communication (including email, text messaging, instant messaging, telephones, computer systems and other electronic records). In addition to the notice provided in this policy, users may also be notified with a warning banner text at system entry points where users initially sign on about being monitored and may be reminded that unauthorized use of the State's IT resources is not permissible.

The SE may impose additional restrictions beyond those set forth in this policy, at the discretion of their executive management, on the use of a particular IT resource. For example, the SE may block access to certain websites or services not serving legitimate business purposes or may restrict user ability to attach devices to the SE's IT resources (e.g., personal USB drives, smartphones).

Users accessing SE applications and IT resources through personal devices must only do so with prior approval or authorization from the SE.

[2] 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 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.

4.1 Acceptable Use

All uses of information and IT resources must comply with State policies, standards, procedures, and guidelines, as well as Executive Orders, any applicable license agreements, and Federal, State, and local laws, rules, and regulations (e.g., intellectual property laws, IRS Publication 1075).

Consistent with the foregoing, the acceptable use of information and IT resources encompasses the following duties:

- Understanding the baseline information security controls necessary to protect the confidentiality, integrity, and availability of information;
- Protecting State information and resources from unauthorized use or disclosure;
- Protecting personal, private, sensitive, or confidential information from unauthorized use or disclosure;
- Observing authorized levels of access and utilizing only approved IT devices or services; and
- Immediately reporting suspected information security incidents or weaknesses to the appropriate manager and the applicable information security officer (ISO)/designated security representative.

For additional details regarding how users must protect State information, see Exhibit A.

4.2 Unacceptable Use

Every user has a duty to properly use state resources in a manner that will mitigate risk to the State, to include mitigating risk of data loss, unauthorized access, acceptance of unfavorable legal terms and conditions, or compromised security of State systems or State information. The following list of unacceptable uses is not intended to be exhaustive; it is provided as a general framework for activities that constitute unacceptable use. Users, however, may be exempted from one or more of these restrictions when acting within their authorized job responsibilities, after approval from SE management, in consultation with SE IT staff (e.g., storage of objectionable material in the context of a disciplinary matter).

Unacceptable use includes, but is not limited to, the following:

- Unauthorized use or disclosure of personal, private, sensitive, and/or confidential information;
- Unauthorized use or disclosure of State information and resources;
- Distributing, transmitting, posting, or storing any electronic communications, material or correspondence that is threatening, obscene, harassing, pornographic, offensive, defamatory, discriminatory, inflammatory, illegal, or intentionally false or inaccurate;

- Attempting to represent the SE in matters unrelated to official authorized job duties or responsibilities;
- Connecting unapproved devices to the State network or any State IT resource;
- Connecting to any wireless network while physically connected to a State wired network;
- Installing, downloading, or running software that has not been approved following appropriate security, legal, and/or IT review in accordance with SE policies;
- Transmitting unencrypted private information, as defined by the Internet Security and Privacy Act, via email;
- Connecting to non-State supported email systems (e.g., Hotmail, Yahoo) without prior management approval (SEs must recognize the inherent risk in using non-State supported email services as email is often used for phishing, distributing malware, or harvesting credentials);
- Using State IT resources to circulate unauthorized solicitations or advertisements for non-State purposes including religious, political, or not-for-profit entities;
- Providing unauthorized third-parties, including family and friends, access to the SE information, IT resources, or facilities;
- Using State information or IT resources for commercial or personal purposes, in support of "for-profit" activities or in support of other outside employment or business activity (e.g., consulting for pay, business transactions);
- Propagating chain letters, fraudulent mass mailings, spam, or other types of undesirable and unwanted email content using State IT resources;
- Tampering, disengaging, or otherwise circumventing NYS or third-party IT security controls; and
- Using State IT resources for personal purposes when such use is not incidental and necessary, is not in a limited amount and duration, and conflicts with the proper exercise of duties of the user.

4.3 Incidental and Necessary Personal Use

Incidental and necessary personal use of IT resources is permitted, provided such use:

- is otherwise consistent with this policy and the requirements of *Executive Order No. 7*[3]*, Prohibition Against Personal Use of State Property*, established June 2008;
- is limited in frequency and duration;
- does not conflict with the proper exercise of duties of the user; and

[3] All references to Executive Order 7 refer to that which was originally issued by Governor David A. Patterson on June 18, 2008, and continued by 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.

- does not impede the ability of the individual or other users to fulfill the SE's responsibilities and duties, including but not limited to, extensive bandwidth, resource, or storage utilization.

Exercising good judgment regarding incidental and necessary personal use is important. SEs may revoke or limit this privilege at any time.

4.4 Individual Accountability

Individual accountability is required when accessing all IT resources and State information. Users are responsible for protecting against unauthorized activities performed under their user ID. This includes locking your computer screen when you walk away from your system, logging off at the end of your work session and protecting your credentials (e.g., passwords, tokens, or similar technology) from unauthorized disclosure. Credentials must be treated as confidential information and must not be disclosed or shared.

Users must ensure their connection of State IT resources is through a known and secured network, such as through the use of a hot spot associated with a state-issued mobile device, or a State-maintained portal that requires user authentication or where the network connection requires a password that is unique to you. A coffee shop or hotel network, for example, that is available for use without these controls is vulnerable to a cyber incident.

4.5 Restrictions on Off-Site Transmission and Storage of Information

Users must not transmit restricted SE, non-public, personal, private, sensitive, or confidential information to or from personal email accounts (e.g., Gmail, Hotmail, Yahoo) or use a personal email account to conduct State business. Users must not store restricted SE information that is non-public, personal, private, sensitive, or confidential on a non-State issued device, or with a third-party file storage service that has not been approved for such storage by the SE.

Devices that contain SE information must be attended to at all times or physically secured and must not be checked in transportation carrier luggage systems.

4.6 User Responsibility for IT Equipment

Users are routinely assigned or given access to State IT equipment to perform their official duties. Users must maintain proper use of the equipment and protect the equipment from theft, damage, abuse, and unauthorized use. Users must never deliberately damage or destroy the equipment or its components. This equipment belongs to the State and must be immediately returned upon request or at the time a user is separated from SE service. Users may be financially responsible for the value of equipment assigned to their care if it is not returned to the SE.

Should State IT equipment be damaged, lost, stolen, compromised, or destroyed, users are required to ipromptly report the incident to their supervisor and SE's Chief Legal Counsel, or the appropriate designated decisionmaker. Prompt reporting here means

within twenty-four (24) hours of discovery, or earlier if possible. Users should consult the SE's Chief Legal Counsel, or their designee, regarding SE legal obligations related to a lost, stolen, or destroyed device and compliance with the Office of the State Comptroller's Guide to Financial Operations Chapter XII.10.E Reporting the Theft, Loss or Misuse of State Assets, if applicable. Users may be subject to disciplinary action which may include repayment of the replacement value of the equipment. The SE has the discretion to not issue or re-issue IT equipment to users who repeatedly lose or damage such equipment.

5.0 Compliance

This policy shall take effect upon publication. Compliance is required with all ITS 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, SEs shall request an exception through the Chief Information Security Office. Details regarding the exception process and the Exception Request Form can be found in ITS Policy, *NYS-P13-001, Information Security Exception Policy*.

Any violation of this policy may subject the user to disciplinary action, civil penalties, and/or criminal prosecution. The SE will review alleged violations of this policy on a case-by-case basis and pursue recourse, as appropriate.

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-P14-001
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: http://www.its.ny.gov/tables/technologypolicyindex

8.0 Revision History

This policy shall be reviewed at least once every two years to ensure relevancy.

Date	Description of Change	Reviewer
01/17/2014	Original Policy Release (*replaces ITS-P05-001 Acceptable Use of ITS IT Systems and NYS-G09-001 Acceptable Use of Information Technology Resources*)	Thomas Smith, Chief Information Security Officer
03/21/2014	Added restriction to section 4.5 for unapproved use of a third-party file storage service for non-public, confidential, sensitive or restricted State Entity information.	Thomas Smith, Chief Information Security Officer
03/20/2015	Incorporated Executive Order 7 into Appendix	Deborah A. Snyder, Deputy Chief Information Security Officer
02/22/2017	Update of contact information and rebranding	Deborah A. Snyder, Deputy Chief Information Security Officer
09/10/2018	Scheduled review – minor change to definition for Information Technology Resources, Authority, Scope, and title of office	Deborah A. Snyder, Chief Information Security Officer
12/07/2018	Revised to clarify State Entity and workforce responsibilities to understand information security controls and to protect State information and resources, and personal, private, sensitive information, from unauthorized use or disclosure. Added an express statement that unauthorized use or disclosure of personal, private, sensitive, confidential or State information is unacceptable.	Deborah A. Snyder, Chief Information Security Officer
01/05/2023	Revised to expressly include a user's duty to mitigate risk to State resources. Added specific reporting requirements related to lost, stolen, or damaged equipment. Moved Use of Social Media section to NYS-P11-001 Use of Social Media Technology Policy.	Chief Information Security Office

9.0 Related Documents

Executive Order No. 7: Prohibition Against Personal Use of State Property and Campaign Contributions to the Governor

NYS-P03-002 Information Security Policy

NYS-P11-001 Use of Social Media Technology

NYS-S14-012 Bring Your Own Device

NYS-S14-009 Mobile Device Security

The following are some examples of physical controls for handling media:

- No confidential information in e-mail subject line, as subject lines are not secure
- SE Privacy disclaimer on e- mail and fax cover sheets
  - SE must include a statement that the contents are intended for the addressed recipient only and must be deleted/destroyed if received in error.
- Reproduction of data outside normal business functions requires authorization by information owner
- Retrieval when printing/faxing
  - Users need to retrieve documents immediately or in a timely manner to protect from unintentional disclosure
- Transportation handling controls for paper both inside and outside the office
  - Hand delivery by State Entity workforce or delivery via courier (e.g., OGS, FedEx, UPS, US Postal Service)
  - Use sealed envelope addressed to specific recipient
  - Where possible obtain receipt confirmation
- Situational awareness during verbal communications
  - Be aware of surroundings when having discussions about HIGH classified information
- If choosing to label paper or portable electronic storage media, use the following: "NYS CONFIDENTIALITY-HIGH", "NYS CONFIDENTIALITY-MODERATE", "NYS CONFIDENTIALITY-LOW". This doesn't replace existing internal labeling structures, but must be included when labeling is used to facilitate the uniform application of controls when information is shared between State Entities. If document is not bound, label each page. Label front and back covers of bound documents.