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:** 12/07/2018
	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 State workforce ("users"). Inappropriate use exposes the State to potential risks including virus attacks, compromise of 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 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*.

3.0 Scope

This policy applies to all "State Government" entities as defined in Executive Order 117 or "State Agencies" as defined in Section 101 of the State Technology Law ("State Entities"), their employees, and all others, including third parties (such as local governments, consultants, vendors, and contractors), that use or access any ITS IT

Resource for which ITS has administrative responsibility, including systems managed or hosted by third parties on behalf of the ITS, hereinafter collectively referred to as "State Entity." Where a conflict exists between this policy and a State Entity'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 State Entities. 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 the New York State Information Security Policy and its associated standards.

4.0 Information Statement

Except for any privilege or confidentiality recognized by law, individuals 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 individuals. Periodic monitoring will 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 State Entity may impose restrictions, at the discretion of their executive management, on the use of a particular IT resource. For example, the State Entity may block access to certain websites or services not serving legitimate business purposes or may restrict user ability to attach devices to the State Entity's IT resources (e.g., personal USB drives, iPods).

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

Acceptable Use

All uses of information and information technology resources must comply with State policies, standards, procedures, and guidelines, as well as any applicable license agreements and laws including Federal, State, local and intellectual property laws.

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 technology devices or services; and
- Immediately reporting suspected information security incidents or weaknesses to the appropriate manager and the Information Security Officer (ISO)/designated security representative.

4.1 Unacceptable Use

The following list is not intended to be exhaustive, but is an attempt to provide a framework for activities that constitute unacceptable use. Users, however, may be exempted from one or more of these restrictions during their authorized job responsibilities, after approval from State Entity management, in consultation with State Entity 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 State Entity in matters unrelated to official authorized job duties or responsibilities;
- Connecting unapproved devices to the State network or any State IT resource;
- Connecting State IT resources to unauthorized networks;
- 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 State Entity policies;
- Connecting to commercial email systems (e.g., Gmail, Hotmail, Yahoo) without prior management approval (State Entities must recognize the inherent risk in using commercial email services as email is often used to distribute malware);

- 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 State Entity IT information, resources or facilities;
- Using State IT information or 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; and
- Tampering, disengaging, or otherwise circumventing NYS or third-party IT security controls.

4.2 Occasional and Incidental Personal Use

Occasional, 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, Prohibition Against Personal Use of State Property; is limited in amount and duration; and does not impede the ability of the individual or other users to fulfill the State Entity's responsibilities and duties, including but not limited to, extensive bandwidth, resource, or storage utilization. Exercising good judgment regarding occasional and incidental personal use is important. State Entities may revoke or limit this privilege at any time.

4.3 Individual Accountability

Individual accountability is required when accessing all IT resources and State information. Everyone is responsible for protecting against unauthorized activities performed under their user ID. This includes locking your computer screen when you walk away from your system, 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.

4.4 Restrictions on Off-Site Transmission and Storage of Information

Users must not transmit restricted State Entity, 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 unless explicitly authorized. Users must not store restricted State Entity, non-public, personal, private, sensitive, or confidential information on a non-State issued device, or with a third-party file storage service that has not been approved for such storage by the State Entity.

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

4.5 User Responsibility for IT Equipment

Users are routinely assigned or given access to IT equipment in connection with their official duties. This equipment belongs to the State and must be immediately returned upon request or at the time an employee is separated from State Entity service. Users may be financially responsible for the value of equipment assigned to their care if it is not returned to the State Entity. Should State IT equipment be lost, stolen or destroyed, users are required to provide a written report of the circumstances surrounding the incident. Users may be subject to disciplinary action which may include repayment of the replacement value of the equipment. The State Entity has the discretion to not issue or re-issue IT devices and equipment to users who repeatedly lose or damage State IT equipment.

4.6 Use of Social Media

The use of public social media sites to promote State Entity activities requires written pre-approval from the State Entity Public Information Office ("PIO"). Approval is at the discretion of the PIO and may be granted upon demonstration of a business need, and a review and approval of service agreement terms by State Entity Counsel's Office. Final approval by the PIO should define the scope of the approved activity, including, but not limited to, identifying approved users.

Unless specifically authorized by the State Entity, the use of State Entity email addresses on public social media sites is prohibited. In instances where users access social media sites on their own time utilizing personal resources, they must remain sensitive to expectations that they will conduct themselves in a responsible, professional, and secure manner with regard to references to the State Entity and State Entity staff. These expectations are outlined below.

a. Use of Social Media within the Scope of Official Duties

The State Entity PIO, or designee, must review and approve the content of any posting of public information, such as blog comments, tweets, video files, or streams, to social media sites on behalf of the State Entity. However, PIO approval is not required for postings to public forums for technical support, if participation in such forums is within the scope of the user's official duties, has been previously approved by his or her supervisor, and does not include the posting of any sensitive information, including specifics of the State Entity's IT infrastructure. In addition, PIO approval is not required for postings to private State Entity approved social media collaboration sites (e.g., Yammer). Blanket approvals may be granted, as appropriate.

Accounts used to manage the State Entity's social media presence are privileged accounts and must be treated as such. These accounts are for official use only and must not be used for personal use. Passwords of privileged accounts must follow State information security standards, be unique on each site, and must not be the same as passwords used to access other State Entity IT resources.

Information posted online on behalf of the State Entity may be subject to the record retention/disposition provisions of the Arts and Cultural Affairs Law and may be subject to Freedom of Information Law (FOIL) requests.

b. Guidelines for Personal Use of Social Media

Staff should be sensitive to the fact that information posted on social media sites clearly reflects on the individual and may also reflect on the individual's professional life. Consequently, staff should use discretion when posting information on these sites and be conscious of the potential perceptions of and responses to the information. It is important to remember that once information is posted on a social media site, it can be captured and used in ways not originally intended. It is nearly impossible to retract, as it often lives on in copies, archives, backups, and memory cache.

Users should respect the privacy of State Entity staff and not post any identifying information of any State Entity staff without permission (including, but not limited to, names, addresses, photos, videos, email addresses, and phone numbers). Users may be held liable for comments posted on social media sites.

If a personal email, posting, or other electronic message could be construed to be an official communication, a disclaimer is strongly recommended. A disclaimer might be: "The views and opinions expressed are those of the author and do not necessarily reflect those of the State Entity or the State of New York."

Users should not use their personal social media accounts for State Entity official business, unless specifically authorized by the State Entity. Users are strongly discouraged from using the same passwords in their personal use of social media sites as those used on State Entity devices and IT resources, to prevent unauthorized access to State Entity resources if the password is compromised.

5.0 Compliance

This policy 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 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. 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.

Term	Definition
Information Technology Resources	Equipment, software, or services used to input, store, process, transmit, and output information, including, but not limited to, desktops, laptops, mobile devices, servers, telephones, fax machines, copiers, printers, Internet, email, and social media sites.

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 12242
Telephone: (518) 242-5200
Email: EISO@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 year 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

Date	Description of Change	Reviewer
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

9.0 Related Documents

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

Secure Use of Social Media Guideline