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:** 02/22/2017 **Issued By:** NYS Office of Information Technology Services **Owner:** Enterprise Information Security Office

1.0 Purpose and Benefits

Appropriate organizational use of information technolog (IT) resources and effective security 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 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 Policy, Standards and Guidelines.*

3.0 Scope

This policy applies to all "State government entities," as defined in NYS Executive Order 117, and to users of any systems, information, or physical infrastructure, regardless of its form or format, created or used to support State government entities.

Therefore, this policy applies to members of the State workforce who are issued or provided access to State information technology resources and covers the use of State information technology resources on any State or non-State network.

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 about this monitoring and reminded that unauthorized use of the State's IT resources is not permissible through the use of warning banner text at system entry points where users initially sign on.

The State Entity (SE) may impose restrictions, at the discretion of their executive management, on the use of a particular information technology resource. For example, the SE may block access to certain websites or services not serving legitimate business purposes or may restrict users' ability to attach devices to the SE's information technology resources (e.g., personal USB drives, iPods).

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

Acceptable Use

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

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

- Protection of confidential information from unauthorized use or disclosure;
- Observing authorized levels of access and utilizing only approved information technology devices or services; and
- Immediately reporting suspected computer security incidents 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 the course of their authorized job responsibilities, after approval from SE management, in consultation with the SE IT staff (e.g., storage of objectionable material in the context of a disciplinary matter).

Unacceptable use includes the following:

- 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;

- Purporting to represent the SE in matters unrelated to official authorized job duties or responsibilities;

- Connecting unapproved devices to the State network or any State information technology resource;

- Connecting State information technology 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 SE policies;

- Connecting to commercial email systems (e.g., Gmail, Hotmail, Yahoo) without prior management approval (SEs must recognize the inherent risk in using commercial email services as email is often used to distribute malware);

- Using State information technology 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 IT resources or facilities;

- Using State information technology 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 information technology resources; and

- Tampering, disengaging or otherwise circumventing NYS or third-party IT security controls.

4.2 Occasional and Incidental Personal Use

Occasional and incidental personal use of information technology resources is permitted, provided such use is otherwise consistent with this policy and the requirements of Executive Order No. 7[1], is limited in amount and duration, and 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. SEs may revoke or limit this privilege at any time.

For example, users may make occasional and incidental personal use of information technology resources to schedule a lunch date, cancel a sports practice, check their bank accounts or other personal investments, or to communicate with a volunteer charity organization.

Your judgment regarding incidental and occasional personal use is important. While this policy does not attempt to articulate all required or proscribed behavior, it does seek to assist in the exercise of good judgment by providing the above guidelines. If you are unclear about the acceptable "personal" use of a state-provided resource, seek authorization from your immediate supervisor.

4.3 Individual Accountability

Individual accountability is required when accessing all IT resources. Each individual 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, including sharing. 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 non-public, confidential, sensitive, or restricted SE 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 non-public, confidential, sensitive or restricted SE 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 SE.

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

---

[1] Executive Order No. 7 **Prohibitions Against Personal Use of State Property and Campaign Contributions to the Governor** states, among other things, that: State computers shall be used only for official business, except that state computers may be used for incidental and necessary personal purposes, such as sending personal electronic mail messages…

4.5 User Responsibility for Information Technology Equipment

Users are routinely assigned or given access to information technology 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 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 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 SE has the discretion to not issue or re-issue information technology 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 SE activities requires written pre-approval of the SE Public Information Office (PIO). Approval is at the discretion of the PIO and may be granted upon demonstration of a business need and review and approval of service agreement terms by SE Counsel's Office, if appropriate. Final approval by the PIO will define the scope of the approved activity, including, but not limited to, identifying approved users.

Unless specifically authorized by the SE, the use of SE email addresses on public social media sites is prohibited. In those instances in which 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 SE and SE staff. These expectations are outlined below.

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

The SE 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 SE. 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 SE's information technology infrastructure. In addition, PIO approval is not required for postings to private SE approved social media collaboration sites (e.g., Yammer). Blanket approvals may be granted, as appropriate.

Accounts used to manage the SE'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 New York State information security standards, be unique on each site, and must not be the same as passwords used to access other SE information technology resources.

Information posted online on behalf of the SE 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 SE staff and not post any identifying information of any SE staff without permission (including, but not limited to, names, addresses, photos, videos, email addresses, and phone numbers). When you choose to post comments on social media sites, you are legally responsible for those comments.

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 SE name or the State of New York."

Users should not use their personal social media accounts for SE official business, unless specifically authorized by the SE. Users are strongly discouraged from using the same passwords in their personal use of social media sites as those used for work, in order to prevent unauthorized access to SE resources in the event that 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 Enterprise Information Security Office exception process.

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 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:

Enterprise Information Security Office
Reference: NYS-P14-001
NYS Office of Information Technology Services
1220 Washington Avenue, Bldg 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

02/22/2017	Update of contact information and rebranding	Deborah A. Snyder, Deputy 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