ANDREW M. CUOMO
GOVERNOR

State Capitol P.O. Box 2062
Albany, NY 12220-0062
www.cio.ny.gov

DANIEL C. CHAN
Acting Chief Information Officer
Acting Director of the Office of IT Services

New York State Information Technology Policy	**No.** NYS-G09-001
IT Best Practice Guideline: Acceptable Use of Information Technology (IT) Resources	**Updated:** 03/25/2010
	Issued By: NYS ITS State Chief Information Officer Director Office of IT Services **Policy Owner:** Security & Risk Management Office

1.0 Purpose and Benefits of the Guideline

Information technology resources are provided by State government entities to employees and other authorized individuals (Users) to assist them with their assigned work responsibilities and duties. Use of such resources is subject to a variety of laws, regulations, executive orders, and policies. Making Users aware of the parameters of acceptable use is an essential part of assuring that the information technology resources are used only for intended purposes and will help mitigate the potential that inappropriate uses will expose the State government entity to unnecessary risks.

Notably, State government entities are, under the provisions of the Information Security Policy (Cyber Security Policy P03-002), required to establish frameworks to initiate and control the implementation of information security. An important aspect of implementing information security is informing employees of applicable information security policies and standards. The purpose of this best practice guideline is to provide guidance regarding the development and dissemination of acceptable use policies for New York State's information technology (IT) resources.

2.0 Scope of the Guideline

Section 2 of Executive Order No. 117 provides the State Chief Information Officer, who also serves as director of the NYS Office for Technology, 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 (IT) Policy, Standards and Guidelines.

This guideline is intended to be of service to all State government entities, as defined in NYS Executive Order No. 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.

3.0 Guidelines

The following acceptable use guidelines are recommended for inclusion in a state government entity's acceptable use policy.

3.1 General

New York State's Information Technology (IT) resources can be separated into two categories: physical assets and information assets. Physical assets are the tangible items, including, but not limited to, workstations, computer print outs, diskettes, and computer servers. Information assets are intangible and include, but are not limited to, passwords, software, and data.

Users are required to protect both types of assets when using the state government entity's IT resources and are responsible for the following:

- Preserving and protecting the IT resources by following all password, protection, and disposal requirements.
- Using the IT resources solely for their intended purposes. Examples of misuse would include viewing inappropriate Internet sites or allowing unauthorized persons to use a state-owned personal computer.

3.2 Guideline Details

Section 1. Individual Accountability

User-ids and passwords must not be shared with **any** person. In addition, users must not:

- Seek to represent themselves as someone else (spoof), obscure, suppress or replace another

individual's identity.

- Access or modify information belonging to others unless the user is authorized to do so by the information owner or the state government entity's Chief Information Officer (CIO).

Section 2. Software and Hardware

Users must not install, attach, or download any hardware or software without prior documented approval from their Chief Information Officer, Information Security Officer, and/or supervisor, as appropriate. Users must follow all procedures required by the state government entity's IT support unit or other authorized software distributing unit in the state government entity. Compliance with such procedures will help prevent infection by computer viruses and ensure that the state government entity and its users do not violate applicable software licensing restrictions.

Section 3. Warning Banner

State government entities must display a warning banner which appears on every user's computer screen giving notice, at a minimum, that the IT resource and all data on it are owned by the state government entity, the uses authorized on the IT resources are for the conduct of the state government entity's business, users have no reasonable expectation of privacy in their use of the IT resources, use may be monitored at any time by the state government entity, and noncompliance with authorized use may result in discipline, including suspension or termination, and/or criminal or civil charges.

A sample warning banner appears as follows:

This system and its applications and data belong to the State of New York. Access and use is limited to authorized users for authorized purposes. Actual or attempted unauthorized use is not permitted and may be a crime subjecting you to disciplinary, criminal, civil, and/or administrative action. You are responsible for any activity attributed to you or your user-ID upon entering this system, and are expected to:

1) Comply with all relevant federal, state, and agency policies, laws, rules, and regulations,

2) Access only systems and information to which you have been authorized for authorized purposes,

3) Not attach or install unauthorized software or hardware to this network or a workstation connected to it,

4) Report any abuse or misuse of this system to the NYS Customer Care Center (1-234-567-8910) and if applicable your supervisor and agency Information Security Officer and cooperate fully in any investigation.

Users have no legitimate expectation of privacy while using this system or any data in it. Any use may be monitored and all information may be accessed, read, copied, used or disclosed by and to authorized personnel for official purposes without additional prior notice to users. This notice shall not be deemed to waive the rights of any person who may be the subject of data in this system. Proceeding with system logon means that you have read and accept the above terms and conditions.

☐ **OK**

Section 4. Acceptable Uses

IT resources are provided to users to assist them with assigned work responsibilities and duties and are intended to be used only for that purpose. Users may use the state government entity's IT resources to:

- Further the State's mission;
- Deliver government services;
- Facilitate business-related research and access to information;
- Provide service of the highest quality to its citizens;
- Discover new ways to use resources to enhance government service;
- Increase staff efficiency; and
- Promote staff development.

Section 5. Prohibited Uses

Users are not permitted to circumvent, probe or test security measures unless such activity is part of their job duties.

Users are prohibited from using the state government entity's IT resources to:

- Write personal communications in a manner that could reasonably be interpreted as official State or the state government entity's policies.
- Conduct outside employment or self-employment activities or engage in private marketing, private advertising of products or services.
- Engage in political activity or solicit for or promote any not-for-profit, religious, political or personal causes.
- View, display or send pornographic or obscene materials. If a user accidentally connects to a site that contains sexually explicit or obscene material, the user must disconnect from that site immediately and report the incident to their supervisor. "Accidental" connections are logged by seconds, not minutes.

- Sign up for personal services, including but not limited to dating or horoscope services.
- Mass distribute any communication, including "chain" letters.

Note: Union use of a state government entity's IT resources is governed by the applicable collective bargaining agreements or side-letters.

Section 6. Personal Use

Personal use of the state government entity IT resources must be consistent with the requirements of Executive Order No. 7.[1] Where personal use of such IT resources has been granted, such use should be permitted only with the restrictions outlined below.

Use must be subordinate and subject to the business needs of the state government entity and not interfere with the conduct of the state government entity's business. Personal use must not interfere or disrupt in any way other users, state government entity's IT resources, network users, services or equipment.

Personal use must only account for an incidental amount of a user's time. An individual has no entitlement to accumulate time to use such IT resources for personal matters. Personal use is restricted to users and does not extend to the user's family members or acquaintances.

Section 7. E-mail

Users should keep in mind that e-mails from a state government entity are visible representations of the government entity and, therefore, New York State. E-mails can be immediately broadcast worldwide and can be received by intended as well as unintended parties. Users can easily mis-address e-mail, and receiving parties can forward e-mail messages to other persons without the original sender's permission or knowledge. Consequently, users should assume that whatever they write may at some time be made public. Accordingly, users should use state government entity IT resources in a legal, professional and responsible manner. All e-mails should include a standard confidentiality/mis-transmission footer approved by the state government entity's counsel.

[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, provided that such use is in a limited amount and duration and does not conflict with the proper exercise of the duties of the State employee.

Only state government entity-approved e-mail products should be used for sending and receiving business e-mails. Use of commercial e-mail systems or Internet service providers (e.g., AOL, MSN) for business e-mails should be prohibited.

Section 8. Web 2.0 and Social Networking

8.1 Government-related communications

Social networking and other Web 2.0 technologies can help drive the state government entity's mission and support professional development. However, improper uses of Web 2.0 technologies raise a number of security and reputational risks and the potential for widespread damage to the state government entity. If use of Web 2.0 and other social networking technologies is permitted by the state government entity, all users must adhere to the following guidelines when using such technologies on state government entity IT resources:

- All policies and work rules apply when participating in a social network or using a Web 2.0 technology for business use. Users are responsible for all of their online activities that are: conducted with a state government entity e-mail address; can be traced to a State government entity's domain; and/or use state government entity resources.
- Users must not discuss or post confidential information.
- Users should be transparent when participating in any online community; disclosing their identity and affiliation with the State government entity.
- Users should communicate in a professional manner
    - Be direct, informative and brief
    - Fact-check posts and include links to source information if possible
    - Spell and grammar check everything
    - Correct errors promptly
- Abide by copyright and other applicable laws. Participation online results in a user's comments being permanently available and open to being republished in other media. Users should be aware that libel, defamation, copyright and data protection laws apply.
- Ensure that the terms of service for social networking sites comply with State laws.
- When communicating on behalf of the state government entity, obtain necessary authorizations by management and the Public Information Officer, or other designee.
- Obtain permission before publishing photographs, videos or quotes of others.

8.2 Personal communications

When not representing the state government entity, users who publish personal or professional opinions must not invoke their state government entity title. In such cases, users must use a disclaimer such as the following where technically feasible: "The postings on this site are my own and don't necessarily represent the position, strategy or opinion of (the state government entity)."

4.0 Definitions of Key Terms

A complete listing of defined terms for NYS Information Technology Policies, Standards, and Best Practice Guidelines is available in the "NYS Information Technology Policies, Standards, and Best Practice Guidelines Glossary" (http://www.its.ny.gov/policy/glossary.htm).

5.0 Contact Information

Submit all inquiries and future enhancements regarding this guideline to:

Policy Owner
Attention: Security and Risk Management Office
New York State Office of Information Technology Services
State Capitol, ESP, P.O. Box 2062
Albany, NY 12220

Questions may also be directed to your ITS Customer Relations Manager at:
Customer.Relations@cio.ny.gov

The State of New York Enterprise IT Policies may be found at the following website:
http://www.its.ny.gov/tables/technologypolicyindex.htm

6.0 Scheduled Revision and Review History

Date	Description of Change
11/05/2009	Original Guideline Issued
03/25/2010	Strengthened Guideline and referenced Information Security Policy (Cyber Security Policy P03-002).

03/25/2012	Scheduled Revision and Review
09/12/2012	Reformatted and updated to reflect current CIO, agency name, logo and style.

7.0 Related Documents

Information Security Policy (Cyber Security Policy P03-002)
http://www.cscic.state.ny.us/lib/policies/documents/Cyber-Security-Policy-P03-002-V3.2.pdf.