



Office of Information Technology Services

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

New York State Information Technology Standard	No: NYS-G10-001
IT Standard: Secure Use of Social Media	Updated: 10/25/2018
	Issued By: NYS Office of Information Technology Services Owner: Chief Information Security Office

1.0 Purpose and Benefits

The primary objective of this guideline is to provide best practices for the secure use of social media for collaboration and transparency in New York State (NYS) government.

Social media, as referred to here, are web-based publishing and communications technologies, such as blogging, social networking, forums, wikis, and file sharing. They are called “social” because they are designed for creating dynamic human networks and exchanging user-generated text and rich media, such as audio and video. They are among the most widely used technologies on the Internet.

Social media hold enormous power for collaboration and communication. Social media carry significant dangers ranging from accidental misuse to intentional criminal abuse. Risks to information and computer systems are significant. The use of social media is ever-changing and therefore the dangers and risks also vary. Information and systems security professionals must be both vigilant and creative in responding to the shifting risk environment.

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* provides the State Chief Information Officer with 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-](#)

3.0 Scope

This guideline is intended to educate 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 Information Technology Resource for which ITS has administrative responsibility, including systems managed or hosted by third parties on behalf of the ITS, on the risks associated with the use of social media, to reinforce the minimum security requirements contained in the [NYS Information Security Policy](#), and to suggest additional mitigating techniques for use of externally hosted social media (e.g., Facebook, YouTube, Twitter) as well as State hosted social media accessible by the public (e.g., wikis, blogs). **This guideline is not applicable to social media designed for internal entity use only, such as an internal wiki or blog.**

This guideline addresses security issues of social media use, not the acceptable use of social media. Use of social media within State government must be in accordance with the [NYS Acceptable Use of Information Technology \(IT\) Resources Policy](#).

4.0 Guidelines

4.1 Security Risks

Cyber criminals target social media sites because they offer an effective means of propagating malicious code to a wide, unsuspecting audience. Sites that allow user-generated content are among the most active distributors of malicious content, such as worms that can shut down networks, or spyware and keystroke loggers that can compromise State data. Many postings to blogs, chat rooms and message boards are spam or contain malicious links. Since many links on social media sites are in the form of shortened or condensed URLs (e.g., TinyURL, Bit.ly), a user is unable to determine where these links lead, making it easy for criminals to direct an unsuspecting user to malicious sites. The false sense of a trusted community when visiting social media sites increases the likelihood that a user may fall victim to this type of threat. If an employee is using State resources when this occurs (e.g., a work PC), these resources have an increased risk of becoming infected.

Many social media sites do not have adequate security controls to protect the information they are holding. For example, some sites do not require strong passwords, some transmit credentials in clear text and some use easily guessed “secret” or “challenge” questions. As a result, social media accounts are frequently compromised. If the same account credentials are used for both the external social media site and State resources, this could lead to unauthorized access to State resources.

By allowing access to externally hosted social media sites, an agency may inadvertently bypass its own security controls. For example, external instant messaging and email services, which may be blocked within an agency because of security concerns, may be accessible through applications available on externally hosted social media sites.

Inadvertent exposure of confidential State information is another risk associated with the use of social media. The ease of posting all types of content (e.g., documents, photos, videos, audio recordings) to social media sites, coupled with the erroneous assumption of a trusted environment, may result in the disclosure of confidential State information.

Use of social media sites leads to a greater web presence, which in turn leads to a greater risk of spam and targeted phishing attacks. Some social media sites harvest information from email contact lists, which may put agency contact information in the hands of a third party with no knowledge of how that third party will use and/or protect that information. Information about a user's professional role in State government, including State email addresses, should not be included on personal profiles. With the wealth of information available on social media sites, hackers are using tools to correlate information into a detailed user profile which can then be used for targeted phishing and other social engineering attacks.

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. Some social media sites may claim to own the content posted on their site. It is important to note that the information conveyed on these sites could be considered a record as defined in the [NYS Arts and Cultural Affairs Law](#).

4.2 Mitigation of Risks

The following recommendations are designed to limit, but will not eliminate, the security risks associated with the use of social media.

4.2.1 Governance and Use

- Use of social media on behalf of a State entity (SE) or access to social media from State resources should be at the discretion of the SE's executive management.
- Authorize use of social media after a proper evaluation of risk and demonstration of a justified business need.
- Develop acceptable use policies to include social media and publicize these policies to users.
- Educate users on SE's acceptable use policy and the risks associated with social media as part of the SE's annual security awareness training.
- Do not use the same passwords for social media sites as are used to access State resources.

- Classify SE data prior to posting per the [NYS Information Classification Standard](#).
- Do not post any non-public SE records (e.g., documents, photos, videos, audio recordings) without following an established SE process, consistent with State and agency policy on information security that includes documented approval from agency management.
- Do not post any personal, private or sensitive (PPSI) information on social media sites.
- Where possible, minimize the posting of information about one's role in State government, including State email addresses, on social media sites.

4.2.2 Technological Controls

- **URL and IP Filtering:** This technology blocks certain websites, parts of websites, or IP addresses. This can help protect users who may be redirected to a known malicious site. In addition, for some social networking sites, using URL filters to block the login pages for all but those employees with a business need, allows for access to public information while preventing access to applications and messaging tools that may bypass a SE's security controls.
- **Malware Filtering at the Network Perimeter:** This technology inspects traffic before it gets into an entity's network to ensure that it does not contain malware and blocks any malware that it finds.
- **Intrusion Detection/Intrusion Prevention Systems:** This technology provides near real time monitoring and analysis of network activity for potential attacks in progress.
- **Data Loss Prevention:** This technology is designed to detect and prevent the unauthorized use and transmission of confidential information. It should be used at both the desktop and the web gateway to monitor for and block outbound confidential data.
- **Browser with Restricted Privileges:** If available, this feature ensures that the browser and its add-ons run with a minimal set of permissions preventing the installation of malicious code.
- **Web Reputation Services:** These services test websites for spam, spyware, scams etc. and use those tests to give safety ratings to help users avoid visiting unsafe sites.
- **Moderating Content:** When hosting a SE social media site, establish a process which would allow the host to moderate (i.e., preview, accept, reject) content submitted to the site prior to its being posted (i.e., made visible to visitors). This helps the host block content containing malicious links or inappropriate content.

- **URL Shortening Preview Tools:** These tools display the actual URL destination masked by shortened URLs from services such as TinyURL and Bit.ly. The preview allows users to make informed decisions about links before clicking.

4.2.3 Policy Controls

State entities must follow all provisions of the [NYS Information Security Policy](#) to facilitate the protection of State information assets, including SE hosted social media sites available to the public (e.g., wikis, blogs), whether on SE infrastructure or hosted at an outsourced provider under contract with the SE. This includes, but is not limited to:

- **Public Website Content Approval Process:** A process must be established for reviewing and approving updates to publicly available content. These reviews must consider the type of information being made available, the accuracy of the information and potential legal implications of providing the information, such as confidentiality and copyright issues.
- **Vulnerability Scanning:** All SE hosts that are or will be accessible from outside the SE network must be scanned for vulnerabilities and weaknesses.

To further protect SE hosted sites, as well as to protect State resources used to access externally hosted social media (e.g., Facebook, YouTube, Twitter), the following controls from the New York State Information Security Policy must also be in place:

- **Protection Against Malicious Code:** Software and associated controls must be implemented across SE systems to prevent and detect the introduction of malicious code.
- **Software Maintenance:** All known security patches must be reviewed, evaluated and appropriately applied in a timely manner to reduce the risk of security incidents.
- **Privileged Accounts Management:** The issuance and use of privileged accounts must be restricted and controlled. Inappropriate use of these account privileges is a major contributing factor to system breaches. Processes must be developed and implemented to ensure that use of privileged accounts is monitored, and any suspected misuse of these accounts is promptly investigated. Passwords of privileged accounts must be changed more often than normal user accounts.
- **Security Incident Reporting:** All staff and contractors are required to report any observed or suspected incidents to the appropriate manager and the SE Information Security Officer/designated security representative as quickly as possible.

5.0 Compliance

This guideline shall take effect upon publication. ITS may amend its guidelines at any time; compliance with guidelines is recommended.

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-G10-001
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 guideline shall be subject to periodic review to ensure relevancy.

Date	Description of Change	Reviewer
05/10/2010	Original Guidance Released (released under the Office of Cyber Security and Critical Infrastructure Coordination (CSCIC))	
05/16/2014	Rebranded for the Office of Information Technology Services (CSCIC/OGS-G10-001 Secure Use of Social Media)	Deborah Snyder, Acting Chief Information Security Officer
05/15/2015	Minor wording changes	Deborah Snyder, Deputy Chief Information Security Officer
02/15/2017	Update of contact information and rebranding	Deborah Snyder, Deputy Chief

		Information Security Officer
--	--	------------------------------

9.0 Related Documents

[NYS Information Security Policy](#)

[NYS Acceptable Use of Information Technology \(IT\) Resources Policy](#)

[NYS Information Classification Standard](#)

[NYS Archives Records Advisory: Preliminary Guidance on Social Media](#)

[CIO Council's Guidelines for Secure Use of Social Media by Federal Departments and Agencies](#)

[Using Social Media in Government](#)