

IT POLICY LETTER

	NUMBER: ITPL 10-02
SUBJECT: SOCIAL MEDIA Emphasis: Secure Use of Web 2.0 / Social Media	DATE ISSUED: FEBRUARY 26, 2010
	EXPIRES: Until Rescinded
REFERENCES: Governor's Reorganization Plan #1 of 2009 Government Code Section 11545 et seq	ISSUING AGENCY: OFFICE OF THE STATE CHIEF INFORMATION OFFICER

DISTRIBUTION Agency Secretaries
Agency Chief Information Officers
Department Directors
Department Chief Information Officers
Department Information Security Officers

PURPOSE The purpose of this Information Technology Policy Letter (ITPL) is to announce:

- The Social Media Standard included in the State Information Management Manual (SIMM) Section 66B.
- Requirements for information technology administrators and management personnel responsible for the technical aspects of Internet connections into agencies.
- Responsibilities for agency¹ heads and program managers related to risk management aspects of enabling network connections to, and the managed use of, social media web sites.
- Changes to the existing State Administrative Manual (SAM) Section 5310 concerning Social Media.

BACKGROUND State agencies are encouraged to use social media technologies to engage their customers and employees. Many state entities, including the Governor, have used these communication channels with great success but as with most technologies, there is a measure of risk that must be addressed and mitigated.

Use of social media falls within two fundamental categories:

- 1) Obtaining information and performing research.
- 2) Sharing or posting official agency information, a two-way flow of information.

¹ When capitalized, the term "Agency" refers to one of the state's super agencies such as the State and Consumer Services Agency or the Health and Human Services Agency. When used in lower case, the term "agency" refers to any office, department, board, bureau, commission or other organizational entity within state government. Within this ITPL, "agency" and "department" are used interchangeably.

The first category should be covered by the agency's acceptable use policy and is not addressed in this ITPL. The second category subjects the agency to the possible exposure of confidential data and is both a cyber security and a business communication issue.

As with any Internet use, agencies must provide protection from cyber security risks associated with the use of social media. However, the specific risk associated with the use of social media technologies centers primarily around the unauthorized sharing or posting of official agency information. This policy and the associated standard directs agencies to apply not only cyber security best practices, but also good business communications practices.

POLICY

Agency heads shall:

- Maximize the use of the government sections of social media sites.
- Ensure that managers and users with access to social media sites are trained regarding their roles and responsibilities
- Assign the responsibility for management and monitoring of social media sites to the individual or entity responsible and authorized for outward-facing communications for the agency.

The responsible individual or entity shall ensure compliance with the agency management requirements and the Social Media Standards included in SIMM Section 66B.

New or expanded use of social media by state agencies shall immediately comply with this policy. Agencies that have already established the use of social media but do not meet the requirements of this ITPL are required to comply by July 1, 2010.

APPLICABILITY

This policy establishes requirements, by reference to SIMM Section 66B, in the SAM Section 5310 for all state agencies, and is applicable to agency heads, agency IT administrators, and social media users.

DEFINITIONS

Social Media - Also referred to as Social Networking and Web 2.0 technologies, are those which allow users to collaborate and share information over the Internet with a network of other social users or the community as a whole (e.g., FaceBook, YouTube, Twitter, MySpace, LinkedIn, Digg, Flickr, etc.).

SAM/SIMM CHANGES

An advanced copy of the updated SAM Section 5310 is included in Attachment A.

SIMM Section 66B is available on the OCIO's Web site at
http://www.cio.ca.gov/Government/IT_Policy/SIMM.html.

CONTACT

Questions concerning this policy should be directed to your CIO, your Chief Information Security Officer, or the OCIO-OIS. Contacts for the OCIO-OIS can be reached at (916) 445-5239 or security@state.ca.gov.

SIGNATURE

/s/

Teri Takai,
Chief Information Officer
State of California

SAM - Chapter 5300

5310 POLICY, STANDARDS, AND PROCEDURE MANAGEMENT (Revised 02/10)

The purpose of information security policy, standards, and procedures are to establish and maintain a standard of due care to prevent misuse or loss of state agency information assets. Policy provides management direction for information security to conform with business requirements, laws, and administrative policies. Standards are the specifications that contain measurable, mandatory rules to be applied to a process, technology, and/or action in support of a policy. And procedures are the specific series of actions that are taken in order to comply with policies and standards.

Each agency must provide for the integrity and security of its information assets by establishing appropriate internal policies, standards, and procedures for preserving the integrity and security of each automated, paper file, or data base including:

1. Establishes and maintains management and staff accountability for protection of agency information assets.
2. Ensure the use of social media technologies is in compliance with the Social Media Standard (SIMM 66B).
3. Establishes and maintains processes for the analysis of risks associated with agency information assets.
4. Establishes and maintains cost-effective risk management practices intended to preserve agency ability to meet state program objectives in the event of the unavailability, loss or misuse of information assets.
5. Agreements with state and non-state entities to cover, at a minimum, the following:
 - a. Appropriate levels of confidentiality for the data based on data classification (see SAM Section 5320.5).
 - b. Standards for transmission and storage of the data, if applicable.
 - c. Agreements to comply with all state policy and law regarding use of information resources and data.
 - d. Signed confidentiality statements.
 - e. Agreements to apply security patches and upgrades, and keep virus software up-to-date on all systems on which data may be used.
 - f. Agreements to notify the state data owners promptly if a security incident involving the data occurs.
6. Establishing appropriate departmental policies and procedures to protect and secure IT infrastructure, including:
 - a. Technology upgrade policy, which includes, but is not limited to operating system upgrades on servers, routers, and firewalls. The policy must address appropriate planning and testing of upgrades, in addition to departmental criteria for deciding which upgrades to apply.

- b. Security patches and security upgrade policy, which includes, but is not limited to, servers, routers, desktop computers, mobile devices, and firewalls. The policy must address application and testing of the patches and/or security upgrades, in addition to departmental criteria for deciding which patches and security upgrades must be applied, and how quickly.
 - c. Firewall configuration policy, which must require creation and documentation of a baseline configuration for each firewall, updates of the documentation for all authorized changes, and periodic verification of the configuration to ensure that it has not changed during software modifications or rebooting of the equipment.
 - d. Server configuration policy, which must clearly address all servers that have any interaction with Internet, extranet, or intranet traffic. The policy must require creation and documentation of a baseline configuration for each server, updates of the documentation for all authorized changes, and periodic checking of the configuration to ensure that it has not changed during software modifications or rebooting of the equipment.
 - e. Server hardening policy, which must cover all servers throughout the department, not only those that fall within the jurisdiction of the department's IT area. The policy must include the process for making changes based on newly published vulnerability information as it becomes available. Further, the policy must address, and be consistent, with the department's policy for making security upgrades and security patches.
 - f. Software management and software licensing policy, which must address acquisition from reliable and safe sources, and must clearly state the department's policy about not using pirated or unlicensed software.
 - g. Ensure that the use of peer-to-peer technology for any non-business purpose is prohibited. This includes, but is not limited to, transfer of music, movies, software, and other intellectual property. Business use of peer-to-peer technologies must be approved by the CIO and ISO.
7. Requiring that if a data file is downloaded to a mobile device or desktop computer from another computer system, the specifications for information integrity and security which have been established for the original data file must be applied in the new environment.
8. Establishing policy requiring encryption, or equally effective measures, for all personal, sensitive, or confidential information that is stored on portable electronic storage media (including, but not limited to, CDs and thumb drives) and on portable computing devices (including, but not limited to, laptop and notebook computers). This policy does not apply to mainframe and server tapes. (See SAM Section 5345.2).

[AUTHORITY](#)

[STANDARDS](#)

[GUIDANCE](#)

[FORMS](#)

[TOOLS](#)