State of California

California Technology Agency

Social Media Standard

SIMM 66B

April 2011

REVISION HISTORY

REVISION	DATE OF RELEASE	OWNER	SUMMARY OF CHANGES
Initial Release	February 2010	OCIO – Office of Information Security	
Updated Office of the Chief Information Officer (OCIO) name references to the California Technology Agency	April 2011	California Technology Agency	

Table of Contents

SOCIAL MEDIA STANDARD

1.0 INTRODUCTION

Agencies[1] and departments are encouraged to use Social Media technologies to engage their customers and employees where appropriate. Many state entities, including the Governor's office, have used Social Media communication with great success, but as with most technologies, there is a measure of risk to address and mitigate. The following requirements will assist in risk mitigation.

This standard is not to be misinterpreted as requiring any state agency to allow the use of Social Media technologies in its environment. Further, this standard does not supersede any existing state agency Social Media policy which exceeds the requirements of this standard.

Note: The Policy Letter provides for a phased implementation of this Standard. See the California Technology Agency's Information Technology Policy Letter 10-02 for details and dates.

2.0 GENERAL AGENCY MANAGEMENT REQUIREMENTS

Prior to authorizing and enabling Internet access to Social Media web sites, agency management shall conduct a formal risk assessment of the proposed connections utilizing agency Risk Management processes. The assessment shall, at a minimum, include the analysis of the risks (including risk mitigation strategies) involved in providing Users access to Social Media web sites including:

1. Employee productivity;
2. Network bandwidth requirements and impacts;
3. Reputational risk to personnel, the agency, and the State;
4. Potential avenue for exposure or leakage of sensitive or protected information such as copyrighted material, intellectual property, personally identifying information, etc; and
5. Potential avenue for malware introduction into the organization's IT environment.
6. The potential use of "other than government" sections of Social Media web sites.

State agencies shall document this risk analysis and retain it for a minimum of two years.

3.0 AGENCY IT ADMINISTRATOR REQUIREMENTS

Agency IT Administrators shall:

1. Limit Internet access Social Media web sites according to the agency's acceptable use policy, while allowing authorized Users to reach content necessary to fulfill the business requirements. Limitations may include:
    a. Opening Internet access only to the government sub-domains on the Social Media web sites.

[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 standard, "agency" and "department" are used interchangeably.

b. Allowing Internet access to Users who are specifically authorized.

c. Preventing unnecessary functionality within Social Media web sites, such as instant messaging (IM) or file exchange.

d. Minimizing and/or eliminating the addition of web links to other web sites, such as "friends", to minimize the risk of exposing a government user to a link that leads to inappropriate or unauthorized material.

2. Enable technical risk mitigation controls to the extent possible. These controls may include:

    a. Filtering and monitoring of all Social Media web site content posted and/or viewed.

    b. Scanning any and all files exchanged with the Social Media web sites.

4.0 USER REQUIREMENTS

1. Users shall connect to, and exchange information with, only those Social Media web sites that have been authorized by agency management in accordance with the requirements within this and other agency and State policies.
2. Users shall minimize their use of "other than government" sections of the Social Media web sites.
3. Users shall not post or release proprietary, confidential, sensitive, personally identifiable information (PII), or other state government Intellectual Property on Social Media web sites.
4. Users who connect to Social Media web sites through State information assets, who speak officially on behalf of the state agency or the State, or who may be perceived as speaking on behalf of an agency or the State, are subject to all agency and State requirements addressing prohibited or inappropriate behavior in the workplace, including acceptable use policies, user agreements, sexual harassment policies, etc.
5. Users shall not speak in Social Media web sites or other on-line forums on behalf of an agency, unless specifically authorized by the agency head or the agency's Public Information Office. Users may not speak on behalf of the State unless specifically authorized by the Governor.
6. Users who are authorized to speak on behalf of the agency or State shall identify themselves by: 1) Full Name; 2) Title; 3) Agency; and 4) Contact Information, when posting or exchanging information on Social Media forums, and shall address issues only within the scope of their specific authorization.
7. Users who are not authorized to speak on behalf of the agency or State shall clarify that the information is being presented on their own behalf and that it does not represent the position of the State or an agency.
8. Users shall not utilize tools or techniques to spoof, masquerade, or assume any identity or credentials except for legitimate law enforcement purposes, or for other legitimate State purposes as defined in agency policy.
9. Users shall avoid mixing their professional information with their personal information.
10. Users shall not use their work password on Social Media web sites.

5.0 RESOURCES

To assist in implementing this standard, additional information and resources are available at the following links.

CIO Council's Guidelines for Secure Use of Social Media by Federal Departments and Agencies - http://www.cio.gov/Documents/Guidelines_for_Secure_Use_Social_Media_v01-0.pdf

Intel Social Media Guidelines - http://www.intel.com/sites/sitewide/en_US/social-media.htm

IBM Social Computing Guidelines - https://www-950.ibm.com/blogs/09100912-b777-4fcf-b726-f28424d9dc44/resource/IBMSocialComputingGuidelines.pdf?lang=en_us

Best Practices for Social Media Usage in North Carolina - http://www.records.ncdcr.gov/guides/best_practices_socialmedia_usage_20091217.pdf

New Media and the Air Force, Air Force Public Affairs Agency, Emerging Technology Division - http://www.af.mil/shared/media/document/AFD-090406-036.pdf