GTA Georgia Technology Authority	**GEORGIA TECHNOLOGY AUTHORITY**	
Title:	**Social Media**	
PSG Number:	GM-11-002.01	**Topical Area:** IT Management, Assess and Manage Risks
Document Type:	Guideline	**Pages:** 4
Issue Date:	June 8, 2011	**Effective Date:** June 8, 2011
POC for Changes:	GTA EGAP	
Synopsis:	Methodology to Employ Social Media	

PURPOSE

The emergence of social media sites using Web 2.0 technologies, such as Facebook and Twitter, gives the State an enormous opportunity to inform and interact with its citizens. Many State agencies have already implemented Twitter and Facebook pages, but most installations of these tools exist only as another way to push information to people, such as a news release. These media can potentially give citizens a new way to talk with government, encourage two-way communication and allow more citizens the opportunity to ask questions and provide input to their government.

The newer tools present yet another risk area for State information and data. This standard outlines the approach that should be followed by agencies which elect to use these media to identify and manage these risks. The approach incorporates industry best practices.

SCOPE AND AUTHORITY

See Information Technology Policies, Standards and Guidelines (PM-04-001) and Enterprise Information Security Charter (PS-08-005)

STANDARD (Referenced State enterprise standards are in brackets and listed at the end of this document)

An agency which uses social media to provide business services shall:

1. Develop an agency strategy (or business case) surrounding the value of social media based services [SM-09-003, SM-10-006, SM-08-103, SM-09-001] and determine what type of service to use, identify how it would be of benefit, what are the costs?

   References:
   1) *"Challenges in Federal Agencies' Use of Web 2.0 Technologies"*, Statement of Gregory C. Wilshusen, Director, Information Security Issues, Testimony Before the Subcommittee on Information Policy, Census and National Archives, July 22, 2010
   2) http://www.archives.gov/social-media/strategies/
   3) http://govsocmed.pbworks.com/w/page/15060450/Web-2-0-Governance-Policies-and-Best-Practices

2. Perform a risk analysis of intended business and technical functions [SS-08-041].
   References:
   1) Legal Risk –
      There is an excellent discussion of legal issues located at
      http://www.inqbation.com/government-policy-on-the-use-of-social-media
   2) Employee Risk –

ISACA offers tips for addressing social media risks.
http://www.isaca.org/About-ISACA/-ISACA-Newsletter/Pages/at-ISACA-Volume18-1September-2010.aspx#1
The Association of Corporate Counsel website summarizes a number of risks associated with employees' use of social media.
http://www.acc.com/legalresources/quickcounsel/wcawesmu.cfm

3) Security Risk –
GSA has a source to review: "*Guidelines for Secure Use of Social Media by Federal Departments and Agencies*", General Services Administration
http://www.cio.gov/Documents/Guidelines_for_Secure_Use_Social_Media_v01-0.pdf

3. Develop a management plan and a security plan [SS-08-028] to operate and to mitigate risks. Possibly a multi-disciplinary team approach which includes business, technology, policy, legal, records, human resources and accessibility stakeholders should be assembled to prepare the plans. A resulting agency plan may include, but not be limited to the following:

A. Terms and Conditions of Use – Agency actions to be taken so that the agency and the State retain protections of existing State laws concerning
    a. Legal constraints on indemnification, and
    b. Venue for potential adjudication.

Notes:
1) Consult legal counsel and State procurement regulations,
2) See negotiated State and Local Government Terms at Facebook:
http://www.facebook.com/terms_pages_gov.php?_fb_noscript=1
3) See content at this link:
https://forum.webcontent.gov/?page=TOS_FAQs

B. Employee access –
    a. Number or type of employees allowed access [SS-08-010],
    b. Acceptable use – Specific authorizations and restrictions on employee personal interests and consequences for violation [SS-08-001].
    c. Social media services approved for access [SS-08-028],
    d. Allowable social media usage [SS-08-041],
    e. Content authorized for posting and/or discussion [SS-08-028, SS-08-010, SS-08-002, SS-08-014],
    f. Logon and off routines, and generic password usage to protect employee personal identities [SS-08-007].

C. Account management – Authorized agency roles in social media account creation, moderation, maintenance and destruction [SS-08-010, SS-08-007].

D. Employee conduct – Ensure that employees are properly trained in social media usage that includes [SS-08-012]:
    a. Awareness of potential security issues and problems [SS-08-012],
    b. Awareness that the employee is a representative of the agency and the State,
    c. Agency imposed limitations on social media usage, such as time of day usage, personal usage, etc. [SS-08-049],
    d. Appropriate on-line identification when using social media on behalf of State versus personal usage [SS-08-007],
    e. Potential risks for violation of Intellectual Property rights of others [SS-08-001, SS-08-009],
    f. Reputational risk to personnel, the agency and the State [SS-08-001],

g. Expectation of appropriate and ethical conduct of a State representative, including cautions against posting offensive, profane, scandalous, libelous, defamatory, pornographic, or otherwise offensive language or materials; and knowing communication of inaccurate or false information[SS-08-001] .

E. Procedures related to inappropriate citizen conduct – Determine how employees and moderators should handle situations when citizens post offensive language or materials [SS-08-049, SS-08-009]. If such posts are pulled from the site, as may be specified by the agency's legal advisor, the agency should save and retain all postings [SS-08-003], both incoming and outgoing as:

a. May be specified by law or regulation

b. They are public records and may be required for subsequent administrative or legal action.

F. Potential for outages – Be aware that the services have a strong potential for outages and plan agency actions for when outages occur [SS-08-045].

G. Reputational risk to personnel, the agency, and the State [SS-08-001];

H. Potential avenue for exposure or leakage of sensitive or protected information such as copyrighted material, intellectual property, personally identifying information, etc [SS-08-049, SS-08-003];

I. Potential avenue for malware introduction into the organization's IT environment [SS-08-033, SS-07-009],

J. Potential use of "other than government" sections of social media web sites [SS-08-001].

K. Provider business models – Service provider business models may change without warning and agency may have to pay for what was previously provided for free [SM-10-006].

L. Advertising and endorsement – Means to limit the agency and its employees from perceptions that they endorse social media advertising, such as inclusion of a disclaimer statement on behalf of the agency and employees (consult legal counsel and State ethics regulations).

4. Prepare and publish a written policy covering your agency's intended use of social media. Ensure that the following topics are addressed:

a. Employee Access

b. Social Media Account Management

c. Acceptable Use

d. Employee Conduct

e. Conduct

f. Security

g. Legal Issues

h. Citizen Conduct

References:

1) *"Online Database of Agency Social Media Policies"*, http://socialmediagovernance.com/policies.php

2) A compendium of policies and best practices assembled by State of North Carolina: http://govsocmed.pbworks.com/w/page/15060450/Web-2-0-Governance-Policies-and-Best-Practices

3) *"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

4) *"Memorandum for the Heads of Executive Departments and Agencies"*, Office of Management and Budget, http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf
5) "*Designing Social Media Policy for Government: Eight Essential Elements*", Center for Technology in Government, http://www.ctg.albany.edu/publications/guides/social_media_policy

GENERAL TOPICAL REFERENCES and BACKGROUND

1) "*Social Media and the Federal Government: Perceived and Real Barriers and Potential Solutions*", Federal Web Managers Council, http://www.usa.gov/webcontent/documents/SocialMediaFed%20Govt_BarriersPotentialSolutions.pdf
2) "*Friends, Followers, and Feeds, A National Survey of Social Media Use in State Government*", NASCIO, http://www.nascio.org/publications/index.cfm
3) "Social Media: Business Benefits and Security, Governance and Assurance Perspectives", ISACA, http://www.isaca.org/Knowledge-Center/Research/Documents/Social-Media-Wh-Paper-26-May10-Research.pdf

RELATED CURRENT STATE OF GEORGIA POLICIES AND STANDARDS

Below are the names and PSG numbers for related PSGs for Georgia. The may be referenced at the following link:
http://gta.ga.gov/00/topic_index_channel/0,2092,1070969_40533560,00.html

a. SM-08-103, "Information Technology Review"
b. SM-09-001, "Project Financial Management"
c. SM-09-003, "IT Strategic Plan"
d. SM-10-006, "Performance Lifecycle Framework"
e. SS-07-009, "Virus and Content Filtering"
f. SS-08-001, "Appropriate Use and Monitoring"
g. SS-08-002, "Classification of Personal Information"
h. SS-08-003, "Data Security Electronic Records"
i. SS-08-007, "Password Security"
j. SS-08-009, "Electronic Communications Accountability"
k. SS-08-010, "Authorization and Access Management"
l. SS-08-012, "Security Awareness and Training"
m. SS-08-014, "Data Categorization – Impact Level"
n. SS-08-028, "System Security Plans"
o. SS-08-033, "Malicious Code Incident Prevention"
p. SS-08-041, "Risk Management Framework"
q. SS-08-045, "Contingency Planning"
r. SS-08-049, "Web and E-Commerce Security"