DEPARTMENT OF ADMINISTRATION
Enterprise Policy

DOIT-10-09-2011

DIVISION OF INFORMATION TECHNOLOGY

Social Networking Policy

Date of Last Revision 02/28/2011

Bijay Kumar
(401) 574-9220
bijay.kumar@doit.ri.gov

1. **Purpose**
   a. To establish guidelines for State agencies, departments, vendors, employees and any individuals with access rights to the State's networks regarding the use of Web 2.0 Social Networking sites, including, but not limited to, Facebook, MySpace, Twitter, Instagram, Reddit, YouTube, LinkedIn and Blogger.
2. **Objectives**
   a. To allow State agencies and departments ("State agency" or "State agencies") the benefit of using Social Networking for the performance of State business, to create a clear distinction between individuals who have view/read-only access to Social Networking sites and those who have the designated authority to post information on State-owned Social Networking sites, to communicate with the public, to protect the infrastructure and legal interests of the State of Rhode Island and to assure that adequate bandwidth is available to conduct State business without interruption.
3. **Scope**
   a. This Policy applies to all State agencies that have been provided access rights to the State of Rhode Island's networks. This includes any vendor, employee, individual or entity that utilizes the networks belonging to the State of Rhode Island and / or State-owned devices such as desktop computers, tablets, or smart phones. Personal use of Social Networking outside of work is also addressed within the Policy.
4. **Limitation**
   a. This Policy is not intended to interfere with rights under the Rhode Island State Labor Relations Act, First Amendment of the Constitution of the United States of America, Article I, Â§ 21 of the Constitution of the State of Rhode Island, or the various whistleblower acts.
5. **Definitions**
   a. Social Networking is defined as any web-based publishing and communications technology such as blogging, forums and Wik.is. As an example, such sites may include Facebook, MySpace, YouTube, LinkedIn, Blogster, Foursquare, Twitter and Flickr.
   b. Social Media is defined as scalable, universally-accessible web and mobile technologies used in the transfer of user-generated content, including conversations and other types of media. Examples of common social media platforms include, but are not necessarily limited to:

(i.) social networks (Facebook, Linkedin);

(ii.) blogs (Wordpress), microblogs (Twitter, Tumblr);

(iii.) social curation (Reddit, Pinterest);

(iv.) media sharing (YouTube, Flickr, Vimeo, Instagram).

c. As there are too many sites to list, any website in this genre is considered "Social Networking." Sites may be hosted by the State or an external entity.

6. Requirements of State Agencies

a. This policy grants State personnel general **read/view-only** access to social platforms and defines the acceptable use of these online resources (Â§ 8. Acceptable media Uses and Mandatory Requirements). However, any State agency or individual seeking promote their State agency or its activities or to gain access for official State business to using a "Social Networking" site, whether hosted by the State or any external entity, must present a valid business case on the "Request for Access to Social Networking Site Authorization Form" attached hereto ("Request") to the Chief Information Officer ("CIO") for review and approval. The Request must be signed by said director or deputy director who will designate responsibility for the creation and maintenance of the site or blog. The statement of a business case will include the reason for the site or blog what advantage the site will attain for the State or its citizens. Users will be limited and to the resources to which they need access. The CIO shall deny, grant or grant with further conditions the Request. Upon approval by the CIO, Information Technology (Office of Chief Information Security Officer "CISO") will establish user access to the applicable social network site(s) and maintain a list of such access that shall include the social network site, individual, user name (if any), email address and password.

b. Upon either (1) termination, contract expiration or for any other reason the access is no longer in use, or, (2) there is a change in authorized user, the supervisor must immediately notify the CIO to terminate and/or change such access.

c. The supervisor or any other person or entity subject to this Policy shall immediately notify the applicable department heads (if any), CISO and CIO of any breach of and/or security or privacy incident under this Policy.

d. Any questions about this Policy should be directed to the CISO and CIO.

7. Statement of Concerns

a. Various sites have differing Terms of Service ("TOS"). In most cases individual sites do not have a custom contract. Therefore, it could be construed that the individual clicking on the "accept" button is agreeing to the terms and not the State of Rhode Island.

b. Many sites have agreements that lack clarity. Always read the TOS carefully. The authorized individual is responsible for reading the TOS.

c. Social Networking sites have been used by criminal hackers to spread malicious programs that can compromise a computer or an entire site. Clicking on links to "see a news story" or "update a Flash Player" have been popular ploys on Social Networking sites.

d. Social Engineering is a danger where a site user becomes "familiar" with a blogger or guest and begins to trust them with information not ordinarily made public. Under no circumstances is a user authorized to provide or make public information deemed confidential by the State.

e. Most social networks do not have adequate security controls to protect the information they are holding. Your password and other credentials are always at risk. Do NOT use the same password for social networking that you use for other State business. To the extent possible, passwords must be configured in accordance with Do IT Policy # 10-01 entitled "Enterprise Password Security".

f. Information posted on Social Networking sites by State agencies, vendors, employees and any individuals with access rights to the State's networks may be construed as an official record and be subject to RI. General Laws § 38-2-1, et seq., as amended titled "Access to Public Records," litigation requests, litigation holds and record retention policies.

g. Caution should be used by public bodies when using Social Networking sites that such use does not constitute an open meetings' violation of RI. General Laws § 42-46-1, et seq., as amended.

8. Acceptable Uses and Mandatory Requirements

a. State personnel are granted **view/read-only** access to Social Networking sites by default in order to:

(i.) View content for purposes directly related to the mission, charter, or work tasks of a State Department or Agency;

(ii.) View content for purposes directly related to the State employee's professional development, to maintain currency of training or education, or to review issues related to the State Department or Agency's official activities;

b. Individuals who wish to create a State-managed Social Networking account and/or post information on any State-managed Social Networking site in an official capacity must first obtain authorization by completing the "Request for Access to Social Networking Site Authorization Form" as outlined in § 6 above.

c. State-managed Social Networking sites may only store, display or include public information in support of the designated State business and must never store, display or request any personal, sensitive or information deemed confidential by the State.

d. **Access and ID's established shall be used solely for State business.** Use of a Social Networking site is subject to compliance with all other State or Agency policies with respect to their electronic communications, including, but not limited to, the Acceptable Use Policy (DoIT Policy #00-02), harassment, discrimination, confidentiality, ethics, workplace violence and other applicable policies and regulations.

e. Forum and chat interfaces are prohibited. (A Facebook-type wall is not considered a forum, but is considered an area for comment.)

f. Default settings on any Social -Networking site should be reviewed and changed to meet the requirements of this Policy.

g. Unless specific authorization is granted by the Request, "Comments" and "Posts" by the public are prohibited, and the settings on the Social Networking sites should be changed to meet this requirement. If an agency has a strong business reason why this function is needed, it should include in its business case the reasons for such functionality, as well as the name of the person(s) who will be responsible for monitoring the comments and posts on a 24/7 basis.

h. If public posting is approved by the CIO, State agency responses to individuals must be made only by an authorized person. Responses must be logged so there is no question as to who responded.

i. Removal of a public comment or post or for a policy or use violation must be approved by the director, deputy director, CISO or CIO.

j. Accounts will be established using a State e-mail account only.

k. The individual designated for such account will insure that no material is used on the site that is in violation of intellectual property or copyright laws.

l. No third-party applications, games or any other information unrelated to State business may be installed on any Social Networking site.

m. All material to be posted on a Social Networking site will be regularly checked for accuracy by the person designated in the Request to ensure that no sensitive, confidential or privileged information is accidently posted. Such checks shall be documented and retained by the State agency for inspection by Legal or the CISO, if needed.

n. Advertisements or endorsements that may be incorporated into a Social Networking site may be prohibited by State procurement or ethics laws. Accordingly, the State agency should try to limit its association by using, or requesting if available, non-branded landing pages and to make sure the linking information provides a disclaimer.

9. Use of Personal Social Networking Sites Outside of Work

a. State personnel are prohibited from using any personal Social Networking application for State business. Any other use shall not reflect or imply he/she is speaking on behalf of or as a representative of the State or Agency, and any views expressed must be the employee's own views.

10. No Expectation of Privacy

a. The State reserves the right to monitor and/or view all Social Networking activity without notice or consent.

b. Any State hardware, software and electronic communication devices such as "Smart Phones" and tablets used for Social Networking, and all communications transmitted through the State network for Social Networking, remain at all times State property.

c. THERE IS NO EXPECTATION OF PRIVACY when using State issued devices or networks.

11. Statement of Enforcement

a. Noncompliance with this Policy may result in one or more of the following actions being taken against the violator:

(i.) Written notification shall be sent to the Agency Head and to the User Agency's Human Resources Liaison and Division of Information Technology Point of Contact to identify the user and the nature of the non-compliance II cause. 11 In the case of an employee or agent of a vendor, sub-recipient, or contractor, the contract administrator shall be notified.

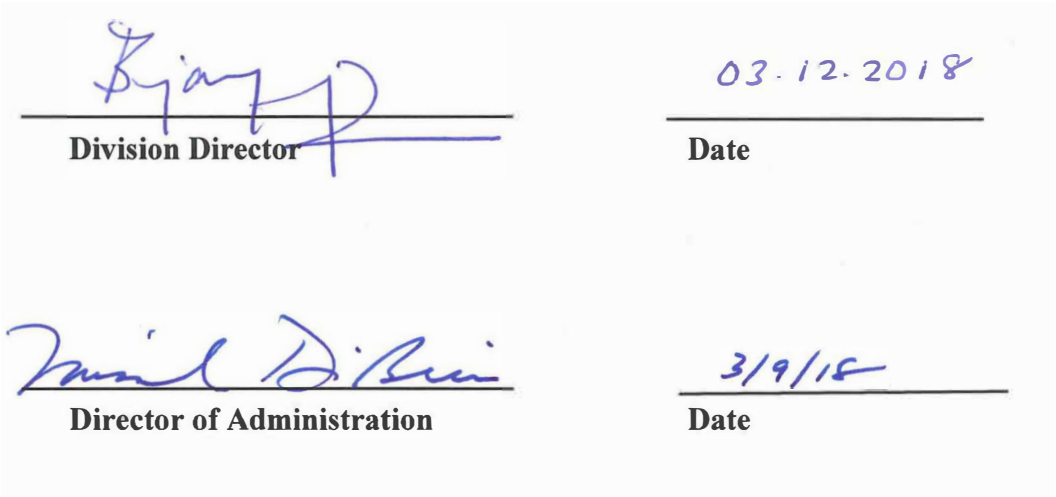
(ii.) User access may be terminated immediately or at any other time deemed appropriate by the CIO or his designee, and the user may be subject to review and corrective action as determined necessary by the agency, department, board or commission leadership, or contract administrator. The termination of the violator's access privileges may be permanent or for a specified period of time as deemed appropriate by the CIO or his designee and the agency, department, board or commission leadership, or contract administrator.

(iii.) Appropriate disciplinary action, up to and including termination, for non-compliance with the terms of this Policy.

12. Rescission, Amendment and Revision

a. The State reserves the right to rescind, amend or revise this Policy at any time.

13. Signatures



ATTACHMENT

State of Rhode Island
Department of Administration
Division of Information Technology

Request for Access to Social Networking Site Authorization Form

1. Access requested to [list site(s)/blog(s)]:

2. Persons that shall have access [list name(s)/title(s)]:

3. The business reason access is being requested, including explanation why intranet or other methods are not sufficient:

4. What benefit shall such access have for the State or its citizens:

5. Discuss the impact on employee productivity:

6. Does the person granted access have the authority to speak on behalf of the Agency? If not, a disclaimer must be added.

7. Will public comments or posts be allowed? If this function is needed, provide the reasons such functionality is required as well as the name and title of the person(s) who will be responsible for monitoring the comments and posts on a 24/7 basis?

8. If a public comment is posted, who shall be designated with the authority to respond [list name/title]?

9. If a comment is posted in violation of the Policy, who shall be designated with the authority to remove the comment [list name/title]?

10. How often will site be reviewed/updated?

11. Who shall be designated with the authority to review/update the site and maintain such records [list name/title]?

12. The Policy on Social Networking read by _____

13. Terms of Service reviewed by _____

ATTACHMENT

Person Requesting Authorization:

Signature:

Name:_____ Title:_____

Agency:_____ Program:_____ Date: _____

Phone Number:_____

Email Address:_____

Cabinet/Department Director Approval:

_____

Cabinet/Department Director
Date:

_____

Recommend Approval/Recommend approval with the following limitations:

_____

Chief Information Security Officer
Date:

_____

Denied/Approved/Recommend approval with the following limitations:

_____

Chief Information Officer
Date:

_____