CONSTRUCTION INDUSTRIES BOARD
Social Networking and Social Media Policy

Construction Industries Board Administrator Approval: November 13, 2015
IT Manager Approval: November 16, 2015
General Counsel Approval: November 13, 2015

State Policy and Standard Specification

The Construction Industries Board (CIB) adheres to the State of Oklahoma Social Networking and Social Media (SNSM) policies found at http://www.ok.gov/cio/Policy_and_Standards/Social_Media/, which include:

1. State of Oklahoma Social Networking and Social Media
2. State of Oklahoma Social Networking and Social Media Development Methodology
3. State of Oklahoma Social Networking and Social Media Guidelines

The CIB implementation of SNSM technologies, approved agency employees using SNSM during the course of agency business and approved agency employees representing the agency on social media in the normal course of business, will adhere to State of Oklahoma SNSM technology toolkits, when published by the Office of Management and Enterprise Services (OMES).

Other Applicable State of Oklahoma Standards

All Web 2.0 and SNSM technologies shall also adhere to the following:

- State of Oklahoma Information Technology Accessibility Standards
- Oklahoma Information Security Policy, Procedures, and Guidelines

CIB Implementation

To protect the position, image and information assets of the CIB, the use of SNSM services is intended for agency purposes only. The CIB recognizes the potential marketing benefits of a SNSM presence and its use is meant to promote and market the mission and goals of the CIB.

Approved agency employees are prohibited from using personal accounts for any state agency related business on any SNSM site. The approved agency employee and the division/business unit manager are to follow all applicable policies and implementation guidelines, and bear the responsibility for any issues caused by an approved employee engaging in the inappropriate use of SNSM technologies.

Use

The CIB Administrator is responsible for overseeing the CIB's brand identity and key messages communicated on the SNSM sites. The CIB Administrator will maintain a log of all SNSM services used by agency employees in the course of official business.

A. The CIB Administrator is responsible for oversight and management of all agency accounts with SNSM providers.

B. Authorization for the engagement with agency SNSM accounts is a function of the CIB Administrator. Written approval from the CIB Administrator is required prior to compilation and publishing using these accounts.

C. Authorized individuals who have obtained written permission from the CIB Administrator must use non-administrative login accounts; and designated workstations should be used to publish content to an OMES-approved SNSM provider.

D. The CIB Administrator will maintain documentation detailing the authorized SNSM service providers, the current account names, the master passwords and person(s) authorized to use the accounts.

The following statements also apply to SNSM usage:

A. All state and agency policies and guidelines pertaining to e-mail also apply to SNSM, including, but not exclusive to, policies regarding solicitation, obscenity, harassment, pornography, sensitive information, and malware.

B. Agency SNSM sites reflect the CIB. Usernames, comments, photos, videos, etc., should be appropriate for a professional environment and selected in good taste.

C. Information published on SNSM sites should comply with the State of Oklahoma Information Security Policy, Procedures and Guidelines.

D. Respect copyright laws and reference sources appropriately. Identify any copyrighted or borrowed material with citations and links.

E. It is inappropriate to disclose or use CIB's, an employee’s or a respective client’s confidential or proprietary information in any form of online media.

F. When representing the CIB in any SNSM activity, the approved employee should be aware that all actions are public and the employee(s) will be held fully responsible for any and all said activities.

G. An approved employee must disclose that he or she is affiliated with the CIB and must respect the privacy of colleagues and the opinions of others.

H. Avoid personal attacks, online fights, and hostile personalities.

I. Ensure material is accurate, truthful and without error.

J. The CIB will ensure comments comply with the Commenting Policy, found in the State of Oklahoma Social Networking and Social Media Policy and Standards.

K. Content that could compromise the safety or security of the public or public systems, solicitations of commerce, or promotion or opposition of any person campaigning for election to a political office or promoting or opposing any ballot proposition shall not be posted to SNSM sites. Content that promotes, fosters, or perpetuates discrimination on the basis of race, creed, color, age, religion, gender, marital status, with regard to public assistance, national origin, physical or mental disability, or sexual orientation shall not be posted to SNSM sites.

L. Do not conduct any online activity that may violate applicable local, state or federal laws or regulations.

Security

SNSM has the potential for security-related issues. Most SNSM traffic is sent in clear text that is not encrypted. The following statements apply to SNSM security:

A. A SNSM service provider and associated plug-ins shall be selected from the applicable sections, policies and standards set forth on the OMES Social Media page.
B. To maintain security of the CIB network usernames and passwords, a SNSM user must use a unique username/password combination that differs from his or her login ID and password for the CIB network.
C. Sensitive information such as usernames, passwords, social security numbers and account numbers passed via SNSM can be read by parties other than the intended recipient(s). Transferring sensitive information over SNSM is prohibited.
D. Peer-to-peer file sharing is not allowed through the CIB network. SNSM clients are prohibited from use of peer-to-peer file sharing.
E. Many SNSM clients provide file transfers. Policies and guidelines pertaining to e-mail attachments also apply to file transfer via SNSM.
F. SNSM can make a user's computer vulnerable to compromise. A SNSM user should configure his or her SNSM account(s) in such a way that messages are not received from unauthorized users.

Escalation

In the event a virus, malware, or any other suspicious activity is observed on the user machine, a user is shall immediately contact either the OMES Service Desk or the CIB service/help desk, as applicable, for prompt assistance to determine the cause of the situation.

Ethics and Code of Conduct

As a state employee Web 2.0 and SNSM technologies are governed by the prevailing ethics rules and statutes.

In addition, all assigned Web 2.0 and SNSM duties are governed by the Oklahoma State Constitution, Oklahoma statutes and applicable rules, and CIB computer usage policies.

Records Management and Open Records

All SNSM communications are subject to the requirements of the Office of Records Management and the Child Internet Protection Act (CIPA). Information about this act and its requirements is found on the Federal Communications Commission (FCC) website

All content, comments and replies posted on any official OMES Web 2.0 or SNSM technology are subject to the Oklahoma Open Records Act. Information disseminated using SNSM technology is subject to being re-printed in newspapers, magazines or online in any other online media format.

Social computing content created or received by state agency personnel may meet the definition of a “record” as defined by state statute, when the content is made or received in connection with the transaction of the official business of the agency, and should be retained as required. This applies to content made or received whether during work hours or on personal time regardless of whether the communication device is publicly or privately owned.

Monitoring

SNSM traffic is logged and reviewed. Logging activity may help in the event an agency account is compromised or improper information is posted to the agency SNSM account.

Logging should at a minimum include the following information:

- Name of user
- Date/Time of use
- User’s activity

Users should have no expectation of privacy. Supervisors may request or be provided reports of Internet usage by employees from the agency information security officer or state chief security officer, as applicable, as needed to monitor use.

Any employee found to have misused or abused a SNSM service or violated this policy may be subject to disciplinary action, up to and including termination of employment.

Communication

The CIB will use SNSM as another tool to connect with media, other agencies and the general public in times of crisis and to assist with emergency, disaster or crisis communications. Information to be published on the agency SNSM sites may include potential delays or closures of sites or services as deemed applicable and prudent by the CIB Administrator.

For assistance with this policy, please contact the OMES Service Desk.