Policy Summary No. 33
Use of Social Media in the B.C. Public Service

Information Security Branch, Office of the Chief Information Officer
Ministry of Citizens' Services, Province of British Columbia
http://www.cio.gov.bc.ca/cio/informationsecurity/index.page

Importance of Information Security

Protection of information assets is the primary goal of information security. This includes practicing safe computing behaviours to reduce the overall occurrence of theft, loss, or misuse of government information assets.

A breach in information security or loss of information assets can have serious consequences, depending on the sensitivity and value of the information and the extent of the breach. The consequences can include: ++

- disclosure of personal information,
- interruption in government's ability to deliver services,
- financial losses related to correcting the situation,
- threats to public safety or individuals' health and well-being,
- legal actions, and
- erosion of the public trust in the government.

Personal action is the

KEY to protecting government information assets. Technology and policies are only effective if personnel are aware of their responsibilities to use the processes enforcing the policies. Education and awareness are essential to promote an understanding of the importance of information security.

The purpose of this document is to provide guidance about security-related aspects of a subject area of interest to the government community. It outlines the subject area background, related security concerns, responsibilities, and relevant information security policy.

This document is for guidance purposes only.

Subject Area Description

Social media has changed the way people communicate. Social media is about participation, conversation and knowledge sharing, and is becoming a powerful tool for both professional and personal purposes. Social media forums are used for communication, collaboration, multimedia, reviews and opinions, entertainment and other information aggregation platforms. Some examples include: LiveJournal, Twitter, LinkedIn, Flikr, Facebook, Digg, YouTube, Yelp.com, WikiAnswers and Second Life.

Social media and collaboration tools create the potential for the Province to speak directly to citizens and communities, and for public service employees to communicate with each other in new and different ways. By doing so, we stand to improve not only communication, but consultation, stakeholder and citizen engagement, policy development and service delivery.

Areas of Concern

The primary area of concern for using social media is the failure to protect information which may be personal, sensitive or confidential and if disclosed may cause damage or harm to individuals or the reputation of government.

Many factors amplify this concern:
- Unauthorized use or disclosure of government information is a security and/or privacy breach. (PS#16 Protection of Sensitive Information)
- Personnel may not be provided with adequate awareness and training regarding sensitive and personal information.
- Personnel may inadvertently post personal information and be in violation of the Freedom of Information and Protection of Privacy Act (FOIPPA).
- Unauthorized use of copyrighted material is an infringement of intellectual property rights.
- When sharing information or providing advice online necessary records may not be captured, retained and filed in accordance with government records management.
- Where personnel use social media sites as a government employee, and wish to provide personal comments on sites, they may contravene the Standards of Conduct and bring the public service into disrepute or be misinterpreted as being an official representative of the B.C. government.

Personnel may incorrectly assume an expectation of privacy for personal, non-work related activity on government systems. All information stored or transmitted on government systems is the property of government.

This Policy Summary offers guidance on using social media and is intended to guide personnel in understanding their responsibilities and obligations according to the Information Security Policy and government standards.

Intended Outcomes

The policies or guidelines associated with the use of social media are intended to:
- Improve awareness of privacy and security considerations when using social media.
- Ensure sensitive and personal information is identified and managed appropriately.
- Ensure personnel are aware of their roles and responsibilities as a government employee when using social media.
- Support appropriate information and records management.

Responsibilities of all Personnel

Things to do:
- Be aware of and understand security policy, standards and guidelines for protecting sensitive and personal information.
- Understand and familiarize with the BC Public Service Philosophy and CISO guidelines on the use of social media.
- Attend information security and social media awareness, education and training opportunities.
- Examine information in view of privacy, intellectual property, records management and confidentiality requirements before making it available on social media.
- Instil confidence and trust and not bring the public service into disrepute.
- Follow your ministry's approval procedure prior to use of social media.
- Involve Public Affairs Bureau when using trademarks or official marks, such as government logos, product brands or other marks.
- Have approval by Intellectual Property Program, Treasury Board or ministry legislative authority where copyright material requires a license.

Things to avoid:
- Engaging in any activity that could be perceived as an official act or representation of government unless authorized to do so.
- Engaging in political activities at work. Employees must be able to retain the perception of impartiality in relation to their duties and responsibilities.

Things to pay attention to:
- Ensure records management practices are understood and followed.

Things to report:
- Actual and suspected security incidents and events as required by the Information Incident Management Process.
- File a General Incident or Loss Report (GILR) within 24 hours of a security incident.

Responsibilities of Management

Things to do:
- Ensure that sensitive and personal information is defined.
- Consult on any suspected or actual information security concerns with the Ministry Information Security Officer (MISO).
- Ensure personnel receive suitable training and regular reminders of privacy and security requirements when using social media.
- When a security or privacy breach has occurred, review and revise related social media policies and processes as needed.

Things to establish procedure for:
- Approval processes where required for any materials being used on social media sites.

Things to be aware of:
- When and how personnel use social media.
- Appropriate use of information and information technology resources by personnel.

Things to reinforce with personnel:
- Adherence to policies, standards and guidelines in using social media.
- Protection of personal and sensitive information.
- Ensure the use of the Information Incident Management Process when required.
- Ensure the staff awareness of the BC Public Service Philosophy and CISO guidelines on the use of social media.

Resources

- Use of Social Media in Government
  https://gww.gov.bc.ca/gov20/social-media
- Records Management, Legislation, Policy and Standards
  http://www.gov.bc.ca/citz/iao/records_mgmt/policy_standards/
- RIM Policy 01-01 - Government Records - http://www.gov.bc.ca/citz/iao/records_mgmt/policy_standards/rim_manual/pol01_01.pdf
- Freedom of Information and Protection of Privacy Act
  http://www.oipc.bc.ca/about/legislation.aspx
- General Incident or Loss Report (GILR)
  http://gilr.gov.bc.ca/
- Information Incident Reporting - Shared Services BC Service Desk at 250 387-7000 or 1-866 660-0811, Select Option 3

References

Document	Description
Core Policy and Procedures Manual http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/CPMtoc.htm	
12	Information Management and Information Technology Management
15	Security
12.3.1	Appropriate Use of Government Resources
18.3.8	Information and Communication
Information Security Policy http://www.cio.gov.bc.ca/local/cio/informationsecurity/policy/isp.pdf	
2.1.5	Confidentiality
3.2.1	Information Classification
4.2.1	Management must ensure personnel comply with policy
4.2.2	Security awareness and training
Standards and Guidelines	
	Social Media Guidelines http://www.gov.bc.ca/citz/citizens_engagement/some_guidelines_master.pdf
	A CISO's Guidelines on the Use of Social Media: Balancing Risks and Maximizing Opportunities http://www.cio.gov.bc.ca/local/cio/informationsecurity/documents/InformationSecurityPerspective_%20SafeUseofSocialMedia.pdf
	Standards of Conduct http://www2.gov.bc.ca/myhr/article.page?ContentID=45bf7662-adf9-8a5f-74f1-657-fedd69edf&dcr=/templatedata/sitepublisher/articles/data/myhr/jobs_hiring/policy09_standards_of_conduct.xml
	Information Incident Management Process http://www.cio.gov.bc.ca/local/cio/information_incident/information_incident_management_process.pdf

Key Contacts

Contact	Link
Office of the Chief Information Officer	http://www.cio.gov.bc.ca/
Information Security Branch, Office of the Chief Information Officer	http://www.cio.gov.bc.ca/cio/informationsecurity/index.page
Ministry Information Security Officer	http://www.cio.gov.bc.ca/cio/informationsecurity/MISO/MISO.page