Guidance for the Secure Use of Collaboration Tools

BACKGROUND

The Government of Canada's (GC) Policy on the Acceptable Network and Device Use (PANDU) recognizes that open access to modern tools is essential to transforming the way public servants work and serve Canadians. This policy requires that public servants have open access to the Internet, including GC and external tools and services that will enhance communication and digital collaboration, and encourage the sharing of knowledge and expertise to support innovation.

Collaboration tools allow public servants to build and maintain interactive dialogue with the communities they serve. Examples include sites such as Twitter and LinkedIn; online presentation sharing tools such as Prezi or SlideShare; and real-time discussion tools such as Slack, to name a few.

CONSIDERATIONS

With public servants increasingly working in the open and accessing new tools, it is important that GC representatives demonstrate good digital literacy skills and good judgment online at all times. From an IT Security standpoint, connections to external tools and services carry the same risks as other connections to the internet. However, departments should take into account that usage of these sites may require some form of identification of the individual and consequently, their association with an organization (e.g. a GC department or agency). In addition, there is a risk that sensitive and protected information could be exposed to the public, either intentionally or unintentionally. Consequently, departments must take in consideration the following:

Cyber security is not just the responsibility of those with cyber security in their job title. It is everyone's responsibility to follow best practices when it comes to cyber security.
Security is everyone's responsibility.

- Posting of information on external tools and web services will likely divulge the origin of the information;
- All information posted on the internet, regardless of the amount of time it is available, is effectively permanently recorded. There are no control provisions for any information once posted;
- The nature of external tools and web services like social networking sites makes them appealing targets for malicious exploitation. These sites are inherently prone to malicious users providing links to malware content that can propagate to a department's infrastructure;
- Content on external tools such as Trello, Slack etc. may be stored on servers located outside Canada thus the content along with associated user metadata can be monitored by non-Canadian and /or third party products, services or businesses;

- Everything that is shared using external tools and web services could be subject to Access to Information and Privacy (ATIP). Public servants must ensure that information related to the mandate of the organisation and/or contains decisions on government activities is properly captured and managed, following information management best practices; and
- Public servants are encouraged to verify data retention requirements when using external tools, in accordance with the TBS Policy on Information Management. Some externally provided tools will retain your information even after you have deactivated your account[1].

All employees are responsible for safeguarding information and assets under their control, to apply security controls related to their day-to-day processes, report security incidents and maintain awareness of security concerns and issues. These tools are to be use for collaborating and facilitating work, not to replace your existing suit of enterprise tools or to bypass security measures. With everyone doing their part to help protect the GC, we will build a stronger first line of defence.

USER TIPS

DO's	DON'Ts
• Protect your identity by using privacy settings on all tools and devices, and limit the amount of information you provide on your profile page. • Use strong authentication mechanisms (for example, multi-factor authentication) where possible to protect from unauthorized access and enable auto-lock of your device. • Use unique passwords for every account, especially separate passwords for personal and work accounts. • Be conscious of what you are sharing and with whom and assume that everything you share could be made public. • Use modern operating systems and web browsers that are maintained with up-to-date software and configured with appropriate host-based protections. • Report any suspicious activity or security incidents so that your departmental security team can address the issue.	• Never share protected or sensitive information, unless you have express consent from your departmental information technology group. • Use caution when opening unsolicited links, attachments, or when prompted to install any software. If you don't know the sender or were not expecting to receive a link or attachment, think twice before opening. • Do not re-use the same passwords that are used for your internal corporate credentials. • Use caution and avoid using untrusted networks or free Wi-Fi. • Never post or share passwords or credentials on web services and tools • Do not ignore SSL certificate errors and unsecure (e.g. HTTP) websites

[1] https://slack.com/privacy-policy

DO's	DON'Ts
• Implement IM best practices and save decisions made using a collaboration tool in your departmental IM repository. • State clearly in your social media profile (used for professional purposes) that your views are your own, not those of your employer. This statement does not absolve you of your obligations or expected behaviours as a public servant.	

ADDITIONAL TIPS

Here are some tip sheets and information on protecting yourself online:

- Public Safety: Get Cyber Safe – Your life online
- CSE: Tip Sheet

REFERENCES

- Policy on Acceptable Network and Device Use (PANDU)
- Direction on Enabling Access to Web Services: Policy Implementation Notice
- Policy on Government Security
- Directive on Departmental Security Management
- Operational Security Standard: Management of Information Technology Security (MITS)
- Information Technology Security Guidance-33 IT Security Risk Management: A Lifecycle Approach
- Communications Security Establishment (CSE) Top 10 IT Security Actions
- CSE ITSB-66 Cyber Security Risks of Using Social Media - Guidance for the Government of Canada
- Policy on Access to Information
- Policy on Privacy Protection
- Guideline on Acceptable Network and Device Use (GANDU)
- Policy on Information Management

ENQUIRIES

For additional information or clarification regarding this document, address inquiries to TBS-CIOB, Cyber Security (zztbscybers@tbs-sct.gc.ca).