Video Communication Platforms

When you can't meet with your coworkers or clients face-to-face, communicating by video can be the next best thing. This brief will help ensure that your use of video communication platforms addresses privacy, security and legal risks.

B.C. legislation and data residency

Video communication platforms that store data outside of Canada generally do not comply with the *Freedom of Information and Protection of Privacy Act*'s data residency provision. However, Ministerial Order 085 allows the use of **third-party applications and tools** to support operations during the COVID-19 public health emergency. In order to use these tools, you must ensure that they are **reasonably secure**, that you make all reasonable efforts to remove personal information as soon as possible when the order expires (June 30, 2020), and that records created using these tools are managed appropriately.

Reasonable security

"Reasonable security" means that the more sensitive the information, the more secure it should be. Evaluate the risks and benefits, consult appropriate parties within your organization, and take steps to ensure your information is reasonably secure before using a video communication platform.

Security best practices and tips

Determine whether you will be sharing *confidential* or *public* information.

- What are the risks if this information is shared beyond the intended recipients?

Choose a service provider with strong security and privacy policies and features.

- Look for proactive privacy and security policies, as well as strong encryption (both in transit and at rest).
- Seek security and legal counsel on the terms of use.
- Know what information the provider will collect.
- Use different passwords and credentials than the ones you use for your work accounts.

Questions?

For ministries and the broader public sector:

Information Security Branch
OCIOSecurity@gov.bc.ca

Privacy and Access Helpline
250-356-1851
privacy.helpline@gov.bc.ca

Set up a secure video conference or meeting.

- Modify the default settings to meet your organization's security requirements.
- Send invitations using email or encrypted messaging apps, never public websites, or social media.

Choose a secure physical setting.

- Host your video conference from a private location.
- Use muting and headphones to prevent confidential discussions from being overheard.
- Remove private information from your background.

Limit and monitor meeting participants.

- Use passwords, user authentication or virtual lobbies.
- Ask phone guests to identify themselves.
- Lock the meeting once all participants have joined.
- Know how to eject unwanted participants or assign a co-host to address security issues quickly.

Provide a collection notice, if required.

- If you will **collect personal information** from participants, then you must notify them of the purpose, legal authority, and point of contact for questions about the collection.
- You should notify participants if the platform or tool stores information outside of Canada.
- **Disclosing personal information** between public bodies does not require a collection notice.

Only share what is appropriate and necessary.

- Ensure only authorized individuals have access to the information you share.
- Limit screen sharing, annotation, or private messaging to avert unauthorized content and other distractions.
- Share an application rather than the entire screen.
- Do not click on suspicious links or attachments.
- Before you upload or share a document, consider whether it is appropriate (e.g. copyright, licensing).
- Notify participants of intended recordings and manage these records appropriately.