Tip Sheet for Work-Related, Government-Approved Foreign Travel

The purpose of this document is to provide guidance and strategies to protect government information and maintain security of this information and your government-issued mobile device, when travelling on government business outside of Canada. Without advance preparation, personal and government information may be at risk if you take your mobile device with you when you travel. Hackers, organized crime, and foreign governments may target you and/or compromise your device to gain access to sensitive data. Government's information and records may be accessed if your device is inspected, confiscated, stolen or lost. The BC Government network and systems may also be at risk if your device is compromised.

Unsure if you are travelling to a known or suspected high-risk country?

Use the Travel Risk Matrix to assess if you need to request a briefing from the Government Security Office (GSO). Also, check with your Ministry Information Security Officer (MISO) first before you travel for work as your ministry MAY NOT allow you to take your government-issued mobile/portable device outside of Canada. You may be asked to take a temporary or surplus smartphone, iPad/tablet, and/or laptop instead of your regular government-issued device, depending on the nature of your work and your travel destination. Travel only with the devices you will need.

Resources

There are several policies and resources that provide specific information you need to be familiar with before you travel:

- Information and technical support specific to pre-travel device setup, wiping of data and technical management of mobile devices can be found via the Mobile Device Management Service (MDMS) Portal. You may also contact the OCIO Service Desk by email or phone at 250-387-7000 (select option 4) for assistance. A list of common device setup questions is also available at OCIO My Service Centre
- For information about appropriate use of your mobile device, please refer to the Appropriate Use Policy (AUP).
- For information about managing confidential information, please refer to the Managing Government Information Policy (MGIP).
- For information specific to Information Security, please refer to the Information Security Policy - Province of British Columbia.
- The Freedom of Information and Protection of Privacy Act (FOIPPA) governs the collection, use, disclosure, storage and access of personal information held by the Province. Except in very limited situations, FOIPPA prohibits personal information by Government from being stored or accessed outside of Canada. More specifically, for employees, the legislation permits you to access personal information while travelling outside of Canada – such as on a laptop or smartphone – if it is necessary to perform your duties or if the information is immediately necessary to protect your health or safety.
- You may contact the Privacy and Access Helpline by email or phone at 250-356-1851 for questions related to privacy and work-related, government-approved foreign travel.

Things to Consider Before You Leave

***Please check first with your MISO as some ministries DO NOT allow employees to take government-issued mobile devices outside of Canada.**

How do I prepare my government-issued mobile devices?

- Set up your devices appropriately in advance:
  - Mobile devices and Mac laptops must to be enrolled with MDMS; and
  - Set up and test VPN or DTS on your devices before travel.
- Backup your devices and remove any unnecessary apps/software.
- Ensure you bring only government information that you will need to work on during your travel.
- Ensure your PIN or password is unique to your device so that when it is compromised, it can't be used to access your other devices or accounts.
- Request your phone coordinator (Admin or local plan carrier) to arrange a mobile-device data travel plan that provides roaming data and cellular services (preferably one that does not require a wi-fi connection).
- Ensure your device settings are configured to prevent unauthorized access to the government network, and to protect against external attacks when connected to public wi-fi networks.
- Follow IDIR and device Password Best Practices, including configuring your devices to lock automatically after a short period of inactivity (no longer than 2 minutes is recommended).
- Ensure your devices are installed with the most up-to-date anti-malware software and security patches.
- Disable unnecessary wireless connections, and other features on your devices that can be used to secretly surveil your activities or movements when you aren't using them, e.g. GPS, Bluetooth, microphone, camera, etc.
- If you will be connecting your devices to a public network, disable auto-sync or 'share' features on your devices to prevent information being compromised.
- Take your own charger cables and power adaptors for your devices. You may also require a country-specific adaptor for regular charging. In case a regular electrical power source will be unavailable to recharge your device, bring an additional battery pack as backup.
- Consider placing decals or other unique visual identifiers on all your devices to allow for easy visual identification.

While Travelling

What should I do to keep government information safe while travelling?

- If you have a smartphone, iPad or tablet, turn it to airplane mode.

- Border officials can require you to provide your PIN or password on your device, and search and possibly copy the contents of your device hard drive. Enter your device PIN or password yourself; do not provide it to them and consider this as an information incident.
- Shield the contents on your device screen and when entering your PIN or password from observation by onlookers.
- If anyone plugs their own device to your device, your device is taken from you, or you lose sight of it at any time, advise your MISO of it upon your return.
- Don’t use public USB charging stations where a charging dock or cable is already provided to charge your device as these may be unsafe to use. Use your own charger cable and power adaptor instead.
- If you need to connect your laptop device to the internet, setup and use a “personal hotspot” with your smartphone instead of using the public hotspot or wi-fi network. If you must connect to a public wi-fi network to work, use the virtual private network (VPN) service installed on your device before your travel, e.g. Cisco AnyConnect, or Desktop Terminal Services (DTS) to connect to government systems and networks.
- Never leave your devices (or your encrypted storage drives unattended). Use your hotel safe (not your room safe) or other secure facilities (e.g. car trunk) to store them if you can’t always carry them on your person.
- Don’t allow others to use your devices.
- Don’t discuss government business on non-government phones and avoid unnecessary communication of sensitive information, including conducting confidential conversations in public places.
- Don’t use gifted devices (i.e. anything that needs to be plugged-in or paired with your device for full use). You may accept them, but they must be examined first by your IT team before use. Contact your MISO who will determine the necessary course of action.
- If you take government information on a government encrypted storage drive and can’t avoid plugging it into a non-government device, don’t use that drive again with your government-issued device. When you return, contact your MISO who will determine the proper course of action.
- Don’t click on links and attachments in unsolicited or suspicious emails/text messages. Be wary of phishing emails/text messages.

What are “information incidents”? What should I do if one occurs?

- An information incident is a single or a series of events involving the collection, storage, access, use, disclosure, or disposal of government information that threaten privacy or information security and/or contravene law or policy. A privacy breach is a type of information incident. Information incidents may occur when:
  - Your account login credentials have been compromised;
  - The security of your device is compromised, for example, by being infected by malware or being successfully hacked; or

  - Your government-issued device (e.g. smartphone, tablet, laptop or storage drive) has been lost, stolen or accessed/seized by a foreign government.
- Report any actual or suspected information incidents immediately as required by the Information Incident Management Policy. Information incidents must be reported to your supervisor and by calling 250-387-7000 (1-866-660-0811). You must also report actual or suspected information incidents to the Risk Management Branch and Government Security Office by completing a General Incident or Loss Reporting Form (GILR) immediately upon your return.

Are there any additional security concerns I should keep in mind?

- Realize that all your communications may be monitored.
- Be vigilant to ensure that you turn off device features such as the microphone, camera, Bluetooth and GPS after use, and be aware others might try to access these features to conduct unwanted surveillance or tracking of your activities.

After You Return

What should I do first when I get back?

- Reset your passwords before accessing government resources or information.
- Ensure all work files that you had saved to your device hard drive (or the government encrypted storage drive if you had used one) during your travel to an authorized government records system.
- If you had reported an information incident during your travel, complete and submit the GILR for it without undue delay.
- Promptly return temporary or surplus devices and submit all gifted devices before use with your government-issued devices to your IT support person so they may be examined for malware. Contact your MISO if you have questions about these.
- Report any suspicious device activity. If you have any reason to believe your device has been tampered with, report this to your MISO.
- Restore your device that you had backed up before departure if required.
- Discontinue your data travel plan.

Contacts

I have a specific question or problem. Who can I contact?

Contact your MISO for further guidance, advice and assistance in interpreting these guidelines.

For more information, see:

- B.C. Government Information Security web page
- Government of Canada Cybersecurity while travelling

- Mobile Device Guidelines