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, 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, compromise your devices and/or try to obtain sensitive data. Government's information and records may be accessed if your device is inspected, confiscated, stolen or lost. The B.C. Government network may also be at risk if your device is compromised.

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

Check with your Ministry Information Security Officer (MISO) before you travel. You may be asked to take a temporary or surplus iPhone, iPad, and/or laptop instead of your regular government-issued devices, depending on the nature of your work and your destination.

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 in the MDMS Self-Service Portal . You may also contact the OCIO Service Desk by email or phone at 250-387-7000 (select option 4). A list of common device setup questions is also available at https://77000.gov.bc.ca/.
- For information about working remotely, please refer to the Working Outside the Workplace Policy.
- For information about managing confidential information, please refer to the Appropriate Use Policy.
- 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* governs storage and access outside Canada. For example, employees can access personal information while travelling outside of Canada – such as on a laptop or smartphone – if it is necessary to perform their duties. 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?

- Travel only with devices you will need, and which have been set up appropriately in advance (i.e. with MDMS) for government work.
- Follow IDIR and device Password Best Practices including configuring devices to lock automatically after a short period of inactivity (no longer than 2 minutes is recommended).
- Ensure devices have updated antivirus and patches.
- Disable unnecessary wireless connections and Bluetooth when not in use.
- If you will be on a public network, disable auto-sync or 'share' features on your mobile device to prevent information being compromised.

- Set up and test VPN or DTS on devices before travel. Backup your device and remove any unnecessary apps and ensure no government information is stored on device hard drives.
- Request that your phone coordinator (Admin or local plan carrier) arrange a mobile-device data travel plan that provides data and cellular services (preferably one that does not require a WiFi connection).
- Do not use USB charging stations while traveling, especially internationally. Airport and ferry charging stations may not be safe to use (i.e. where a charging dock or cable is already provided). Bring an additional battery pack to charge your devices in case a regular electrical power source is unavailable. You may also require a country-specific adaptor for regular charging.
- If, in extenuating circumstances, you need to store and transport information electronically, ensure you have a government-issued encrypted USB drive. This is useful in case you need a backup of important material. Consider decals or other unique visual identifiers on your devices to allow for easy identification.

While Travelling

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

- Border and airport officials may require you to enter your PIN or password on your device. Protect screens from onlookers and shield passwords during entry. If your device is taken from you or you lose sight of it, alert your MISO upon your return.
- Ensure device settings are configured according to policy to prevent unauthorized access to the government network, and to protect against external attacks if accessing public, guest, and hotel WiFi and internet (i.e. use a "personal hotspot"). Use VPN or VDI (Virtual Desktop Infrastructure) to connect to government systems and networks.
- Never leave devices unattended. Use hotel safes or other secure facilities to store them and do not allow others to use your device.
- Do not discuss government business on non-government phones and avoid unnecessary communication of sensitive information, including confidential conversations in public places.
- Do not click on links and attachments in unexpected or suspicious emails.
- Do not use gifted devices, CDs, or DVDs. You may accept them and bring them back but they must be examined before use and may be wiped upon your return. Contact your MISO who will determine the proper course of action. If you take government information on an encrypted USB drive, and cannot avoid plugging it into a non-government computer, do not use that USB drive again in your device. When you return, contact your MISO who will determine the proper course of action.

What are "information incidents"? What should I do if one occurs?

- Information incidents are when unwanted or unexpected events threaten privacy or information security. They can be accidental or deliberate, and include the theft, loss, alteration or destruction of information. Information incidents may occur when:
  - The security of your device is compromised, for example infected by a virus or successfully hacked;
  - Your mobile device (e.g. Smartphone or Tablet), which has access to your government email account, has been lost or stolen;

- You must report any actual or suspected information incidents immediately by following the Information Incident Management Process. You will be required to call 250-387-7000 (1-866-660-0811) and select Option 3. Ask for an Information Incident Investigation.

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

- Realize that all of your communications may be monitored.
- Be vigilant to ensure that you turn off device features such as microphones, cameras, 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?

- Promptly return temporary or surplus devices, and submit gifted USB drives before using, to your IT support person so they may be wiped. Contact your MISO if you have questions about these.
- Report any suspicious device activity. If you have any reason to believe your device may have been tampered with, report this to your MISO.
- Reset your passwords before accessing government resources or information.
- Restore data you backed up before departure.
- Discontinue your data travel plan.

Contacts

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

Contact your Ministry Information Security Officer 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