Mobile Device Guidelines for BC Public Service Employees

Mobile devices used in the Government workplace to conduct work, such as smartphones, tablets, and laptops, may also be used in uncontrolled public environments, and may easily be lost, stolen or damaged. While mobile devices allow employees to communicate and perform their duties remotely, they pose more privacy and security risks than desktop computers used in secure office spaces.

The purpose of this document is to provide employees with guidance to minimize the privacy and security risks unique to the use of government-issued mobile devices for work based on current legal requirements, government policy, and best practices. It addresses many of the most asked questions employees have about their mobile device use and management.

Many of the key requirements applicable to government-issued mobile devices come from the Appropriate Use Policy (AUP) and the 6.15 Mobile Device Security Standard (see IM/IT Standards). Employees must review the AUP at the commencement of their employment, when they are issued a new mobile device, and annually if they work with a significant amount of confidential information. Employees are expected to adhere to their ministry specific policies or guidelines related to mobile device use.

Your New Mobile Device

1. I have just received a new mobile device. What is the first thing I need to do to set it up properly?

If it is a smartphone, iPad, Android tablet or macOS based device, you must enroll it in the Mobile Device Management Service (MDMS) to access corporate email, calendar, and business applications on your device. You will receive an email with detailed instructions on how to install the MDMS application and complete the enrollment process.

There are only limited circumstances for when a smartphone or tablet , doesn't need to be enrolled in the MDMS – these are specified in the Mobile Device Security Standard. An employee owned personal mobile device of any kind can't be enrolled in the MDMS at this time.

You will also need to choose a strong password (or PIN) for your government-issued mobile device. There are a few password best practices to keep in mind when creating a strong password:

- Choose a password (or PIN) that is difficult for someone else to guess, but easy for you to remember;
- Choose a password (or PIN) that is at minimum 10 characters in length if your device is enabled for it, or minimum of 6, if it isn't; and
- Your password should contain a combination of numbers, symbols, upper- and lower-case characters.

Refer to the Access Control Security Standard for more details on password requirements.

2. How do I protect my mobile device and the information on it?

- Set up the approved authentication features (e.g. passcode, biometrics, etc.) on your government-issued mobile device to unlock it.
- Don't store your logon credentials, password (or PIN) or your device access token (if you were provided one) with your government-issued mobile device. For example, don't tape your password to your government-issued mobile device.

- Never share your logon credentials or password (or PIN) with anyone, e.g. your supervisor, your assistant, technical support, law enforcement, etc., and make sure no one can see your logon credentials or passcode (or PIN) as you enter it.
- Don't reuse your government account (IDIR) password with other accounts, especially with your personal online accounts.
- Ensure that all apps/software on your government-issued mobile device are up to date unless advised otherwise - the OCIO may sometimes advise you to delay/not install some app/software updates.
- Don't allow friends, family members or other third parties to use your government-issued mobile device.
- Don't disable the automatic lock on your government-issued mobile device and always lock it if you must leave it unattended.
- Don't pair non-ministry-issued Bluetooth devices with your government-issued mobile device; disable the Bluetooth function on your device when not using it.
- Don't plug non-ministry-issued USB devices to your government-issued mobile device.
- Only plug trusted charger cables and power adaptors to your government-issued mobile device.
- Never plug your government-issued mobile device into a public USB port.
- Be cautious about opening file attachments or clicking on web links in emails.
- Be cautious about clicking on web links or file attachments in text messages.
- Be cautious about which internet websites you visit on your government-issued mobile device.
- If you can't always carry your government-issued mobile device with you, secure it in a locked drawer/cabinet/with a computer lock cable or when travelling, in your car trunk or use the hotel front desk safe (not your hotel room safe).

Using your Mobile Device

3. Can I use a government-issued mobile device for personal purposes?

Your use of your government-issued mobile device for personal purposes must be reasonable under the AUP and consistent with the Standards of Conduct. This means that you must never use it for illegal purposes or personal financial gain. During work hours, your personal use must be limited, and not interfere with your job responsibilities or compromise the security of your device.

Please be advised that the BC Government isn't responsible for any loss of your personal information (e.g. personal photos, notes, etc.) stored on your government-issued mobile device when it needs to be reset or wiped.

4. Can I store government information on a mobile device?

You must always store government electronic records in protected government systems, for example, the BC Government shared file and print system. All government records saved to the local hard drive of your government-issued mobile device, except emails, must be transferred to a protected government system at the earliest opportunity to ease FOI searches, and be erased from your device.

The AUP outlines what your responsibilities are with storing government information.

5. What if I need to work from home?

You can connect your government-issued mobile device to your home network when working from home. Use Virtual Private Network (VPN) or Desktop Terminal Services (DTS) to access government applications and

systems; e.g. work email, Skype, MS Teams, etc. Use of your personal computer to access government applications and systems isn't recommended. If you must, due to extraordinary circumstances, use only DTS to access them.

6. I regularly work outside of the workplace, including in public places - how can I protect my mobile device?

Carrying and using your government-issued mobile device in public spaces poses a greater risk of exposure to government information. When working outside of the workplace, take appropriate precautions to safeguard the information. In addition to the tips provided in QA #2 above, here are a few more tips to protect your government-issued mobile device and the information you are working with:

- Don't leave your device unlocked or unattended in a public place;
- Make sure others can't observe what you are working on, or your device password (or PIN) or IDIR logon credentials when you enter them; and
- Find a private place where you can't be overheard for work-related phone calls or online work meetings.

7. Can I connect my mobile device to a public wi-fi network?

Never allow your government-issued mobile device to automatically connect to an unknown public wi-fi or hotspot network to connect to the internet. If you must connect it to a known public wi-fi or hotspot network for work, use VPN or DTS to securely logon to government applications and systems. Even connecting your government-issued mobile device to a known public wi-fi or hotspot network presents a high security risk.

An alternative to using public wi-fi networks is to create your own personal hotspot network with your government-issued smartphone that has a data plan and then connecting your government-issued laptop/tablet to it. This uses your smartphone data network and makes it less likely that any information you transmit or receive will be intercepted by a third party. Contact 7-7000 for assistance with setting up a personal hotspot.

8. Can I download new applications or software onto my mobile device?

According to the AUP, you must have your supervisor's permission to download and install additional applications or software to your government-issued mobile device. Before downloading any application or software ask yourself the following questions:

- Is the application or software from the BC Government supplied App Store/Software Centre, Apple's App Store, Google Play Store, Microsoft Store or Microsoft AppSource?
- Is it prohibited by the Office of the Chief Information Officer (OCIO)?
- Would the use of the application or software present unacceptable privacy or security concerns? Use the Applications and Software Guide to determine this; and
- Does it impose terms and conditions that are unacceptable to Government, such as indemnification clauses?

If you are unsure of the answer to any of the above questions or the answer is a yes to any one of them, you must not download or use the application or software.

Supervisor permission is also required if you want to download and use an application or software from the BC Government supplied App Store/Software Centre for a purpose that is different from its original approved purpose.

This isn't meant as a deterrent from downloading useful applications or software, but for both you and your supervisor to become aware of both the benefits and potential risks when using applications or software not made available through the BC Government supplied App Store/Software Centre for government work.

There are also legal restrictions against storing personal information on servers outside of Canada. This can be a problem if you use applications or software for government work that may access information like contacts, calendar info and/or other government records stored such on your government-issued mobile device and transmits that information to a location outside of Canada for processing, for example, Google Docs or Dropbox.

9. Is there a process I need to follow to download a new application or software to my mobile device?

If the application or software to be used for government work isn't available through the BC Government supplied App Store/Software Centre, your supervisor can use the Applications and Software Guide to determine if a privacy and security risk assessment must be completed before it is downloaded to your government-issued device.

Your supervisor can contact your Ministry Information Security Officer (MISO) and/or Ministry Privacy Officer (MPO) for assistance. Once your supervisor has approved the use of the application or software, you can obtain it through the Self-Serve Centre, iStore process or your ministry/office's procurement process. Contact your ministry IT department for assistance with installing the application or software on your device.

10. As an employee, do I need to update or apply patches for the applications or software on my mobile device on a regular basis?

You must apply all application and software updates and patches on your government-issued mobile device yourself unless otherwise advised by the OCIO. This must be done on a timely basis. If your mobile device is a laptop, the OCIO will issue automatic updates and patches for standard corporate applications and software installed on it.

You must also promptly apply all updates issued by the application or software developer for an application or software that you yourself have installed on your government-issued mobile device. You must delete any application or software you no longer use, that has been banned by the OCIO or is no longer supported by the software developer.

11. Am I allowed to change the operating system or security settings on my mobile device?

You must never tamper with the operating system and system security setup on your government-issued mobile device as you could seriously compromise its security.

Traveling Abroad

12. I am travelling outside of Canada for work. Can I take my mobile devices with me?

Check first with your Ministry Information Security Officer (MISO) as your ministry MAY NOT allow you to take your government-issued mobile device outside of Canada.

It is preferred you don't take your government-issued mobile device with you when you travel abroad. If your ministry does permit it, there are several precautions you should take, both *before* and *during* your trip:

- Complete a risk assessment on traveling with your mobile device and the government information that will be on it;
- Follow the advice provided in the risk assessment to mitigate the identified risks; and
- Refer to the Foreign Travel Tip Sheet for specific guidance and strategies to protect government information while travelling.

13. Are there privacy concerns with accessing personal information while travelling?

Please see the Foreign Travel Tip Sheet.

Loss and Disposal

14. I have lost my mobile device! What should I do?

Given the potential for confidential information, including personal information, to be stored on your mobile device, the loss of your government-issued mobile device is considered an "information incident." Report its loss immediately to your supervisor and by calling 250-387-7000 (1-866-660-0811) as required by Information Incident Management Policy. Also report the loss *within 24 hours* to the Risk Management Branch and Government Security Office by completing a General Incident or Loss Reporting Form. You must report the loss of your device without delay and not wait a few days in hope that it will turn up.

15. What is the proper way to dispose of old mobile devices?

Contact your IT Asset Management contact or Records Management Officer for your ministry/organization. They will have policies and procedures to assist you in the disposal of your old mobile devices. Please go to the KB0030886 article in the OCIO My Service Centre website and Asset Disposal Process website for more information on the disposal of mobile devices.

Further Information

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

For general questions about AUP policy requirements and your responsibilities as an employee, please email IM.ITpolicy@gov.bc.ca. For questions specifically about privacy and your mobile device or privacy generally, please contact the Privacy Helpline at 250-356-1851 or privacy.helpline@gov.bc.ca.

For technical support and help with your government-issued mobile device, please call 250-387-7000 or email 77000@gov.bc.ca.