Protect your Mobile Device

(and the information they contain)

Today's mobile devices - laptops, netbooks, smart phones, USB keys (thumb drives), iPods and other mobile devices - are powerful, store large amounts of information, are small, portable and are very easily lost or stolen. Thousands of mobile devices are lost or stolen every year. We use mobile devices in uncontrolled locations such as hotels, airports and other public places and need to be aware of the risks to the devices and the information they contain.

The loss of a mobile device can lead to significant security and privacy issues when sensitive and/or personal information is stored on the device. The device can be, in most cases, quickly replaced but the information that is stored on the device may be invaluable and irreplaceable or used for malicious or criminal purposes. The protection of information stored, transmitted and processed when using mobile devices, requires extra awareness and vigilance in order to protect and secure both the device and the information. Learn about security risks and threats so that you can better protect your device and the information stored on it. The Working Outside the Workplace Policy provides direction to BC Public Service employees on how to safeguard electronic and paper-based confidential and/or personal information when working remotely; this document is a must read for anyone who works 'outside of the workplace'.

Be Aware:

- Take the time to learn and use the security settings on your mobile devices.
- Do not allow the device to automatically connect to an unknown wireless connection (unknown security settings may open the device to hacking or malicious programs).
- When using wireless connectivity features (e.g. 802.11, 802.16, Bluetooth) ensure the security settings are set to be as strong as is reasonable and that you are notified of a connection being made.
- Never leave the device unattended.
- Lock down mobile computers with a locking cable.
- Use in-room safes or other hotel secure facilities to store your mobile devices.
- Carry your portable device in an inconspicuous bag. Flashy, branded or logo bags and expensive cases draw attention to your device.
- Use encryption and/or password protection security features.
- Use a strong password. Create passwords that are tough for hackers to crack, but easy for you to remember.
- Backup your information before you travel. You can't always avoid the financial loss of your equipment, but you can avoid losing all your information.
- Never send/receive sensitive data over a wireless connection unless encryption technology is being used.
- Be aware of the people around you. Shoulder surfing is a common direct observation technique used for information theft.

	**Tips When Flying With Your Laptop** • Conceal your computer in a laptop backpack or another inconspicuous case that doesn't appear to be storing a laptop. • When your laptop goes through the scrutiny scanner at the airport, pick it up as soon as it emerges from the scanner. • On board, store your laptop in the seat pocket in front of you or under your seat, instead of in the overhead compartment.
	**Things To Keep In Mind** • All the encryption in the world won't help if your laptop carrying case gets stolen and it contains plain text copies of sensitive or personal information on CDs, USB keys or on paper. • Locking devices are useless when mobile computers aren't actually locked down with them. • The strongest password is almost useless when it is written down and easily found. (Like a sticky note on or next to the computer or on your business card in the carry case!) • All encrypted data can be permanently lost if you lose the 'key' or passphrase. Decryption keys locked in safes, safety deposit boxes, or otherwise stored in a safe location can help prevent a data loss catastrophe. • Downloading free software from the Internet without a high level of assurance that the product is safe (no adware, no spyware, no viruses) is putting your device and your information at risk.

For more information

Working Outside the Workplace Policy
http://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/working-outside-workplace

Information Security Policy (ISP) – Chapter 7.3 – Access Control – User Responsibilities
Chapter 7.7 – Access Control – Mobile Computing and Networking
http://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/information-security-policy

Hotel Business Centers, How Safe Are They?
http://antivirus.about.com/od/securitytips/a/bizcenters.htm

Using Your Laptop at Starbucks – Is it Safe?
http://antivirus.about.com/od/wirelessthreat1/a/starbucks.htm

Microsoft Windows instructions for backing up information on your computer
http://www.microsoft.com/protect/yourself/data/backup.mspx

Hot Spot Security - Before You Use a Hot Spot
http://mobileoffice.about.com/cs/findinghotspots/bb/byusehotspot.htm