Yukon Information and Privacy Commissioner
201-211 Hawkins Street, Whitehorse, YT Y1A 1Y3 • www.ombudsman.yk.ca • Phone (867) 667-8468 • Fax (867) 667-8469

Fact Sheet

Privacy on the Go: 10 Workplace Tips for Protecting Personal Information on Mobile Devices

Mobile devices such as smart phones, laptops, tablets and USB keys have rapidly become standard tools in business environments. They offer tremendous convenience by allowing employees to keep up with work while out of the office. However, they also raise important new risks for privacy and the protection of personal information.

Mobile devices are increasingly powerful and can hold massive amounts of personal data. They are also small, which means they are easy to lose – or steal. Like desktop computers, they are also vulnerable to threats such as viruses and spyware.

Once personal information is compromised, you can never really get it back and it can be used in ways that could cause significant personal and financial harm.

Organizations must take steps to mitigate the risks – just as they would product computer systems and databases at the office – to ensure that mobile devices do not become the source of a data breach.

A key step is to develop a comprehensive policy on removing personal information from the office – be it on a laptop, a smart phone, a thumb drive or other mobile device. A good policy should address issues such as training; minimizing personal data on devices; and the use of strong security measures to protect any personal information that leaves the office.

10 Tips for Protecting Privacy

1. Ensure that employees understand both their responsibility to protect personal information and the steps they must take in order to do so.

RISK: The best policy in the world will not prevent a data breach unless employees know what it says and understand both how to put it into practice, and why it is important to do so.

2. Limit the personal information that is stored on mobile devices to that which is absolutely necessary. Further protect personal information that leaves the office by de-identifying it wherever possible.

RISK: Personal information can be more vulnerable when it leaves the office. Minimizing the data on a mobile device will reduce the risk.

3. Ensure that mobile devices are protected with hard-to-guess passwords. (For example, use at least one capital letter, both numbers and letters and a special character such as a punctuation mark.) Never rely on factory setting passwords. Use an automatic lock feature so that a password is required to access information on mobile devices.

RISK: Weak passwords – birthday, spouse's or children's names or commonplace words – can be easy to crack.

4. Use an up-to-date encryption technology to protect personal information on mobile devices.

RISK: Without encryption, personal information is vulnerable to unauthorized access. Encryption involves using an algorithm to transform information into text that is unreadable without a "key" to read the code.

5. Install and run anti-virus, anti-spyware and firewall programs on mobile device – and keep those programs up-to-date.

RISK: Attacks against mobile devices – from spam, viruses, spyware and theft – are on the rise. For example, downloading an infected program could infect a mobile device.

6. Ensure that employees don't send personal data over public wireless networks – at cafés, for example – unless you have added security such as a Virtual Private Network (VPN).

RISK: Public wireless networks may or may not be secure and there is a risk that others may be able to capture data sent over these networks.

7. Take steps to ensure that employees are using secure networks if they take work home with them.

RISK: Unless an individual has some IT expertise, a home environment is likely to be less well protected than computers and networks at the office.

8. Remind employees never leave mobile devices unattended in a public place or a vehicle.

RISK: Across North America, hundreds of thousands of mobile devices are lost or stolen every year. One survey by an information security and privacy research centre suggest that a laptop has a 5 to 10 per cent chance of going missing over a three-year period.

9. Establish control mechanisms to ensure that data stored on surplus mobile devices is purged prior to disposal.

RISK: Surplus mobile devices can represent a significant privacy risk if they are not wiped of data.

10. Seek expert advice. These tips are intended only as an introduction to protecting personal information in a mobile workplace.