Office of the Chief Information Officer Directive: IT 14.11	Issued: 04/2020 Last
Chapter: Mobile Device Management	Review: 01/2024
Subject: Securing Mobile Devices When Travelling	

1 DIRECTIVE

1.01 GNB employees in all parts of government that travel outside the work place are responsible to safeguard assigned GNB technology devices and information.

Mobile devices include, but are not limited to:

- Laptops
- Tablets / Notebooks
- Cell phones / PDAs / Blackberries
- USB Sticks / Flash Drives / External Hard drives

2 PURPOSE

2.01 The purpose of this directive is to ensure that government information remains protected while employees are travelling outside the workplace.

3 SCOPE

3.01 This Statement of Directive and Procedure applies to all persons who access GNB resources and information with GNB mobile devices during authorized out of Province travel.

Note: GNB devices must not be utilized during out of Province personal travel.

4 RESPONSIBILITY

4.01 GNB employees (or their management) must advise the DISO (departmental information security officer) and the Information Technology Service Delivery Organization (IT SDO) of any out of Province travel plans, at least three (3) weeks prior to the date of departure. IT SDO will share this information with the appropriate DISO and others as appropriate to ensure they are available to support the traveller.

4.02 GNB employee (traveller) is responsible to

Before travel

(a) review pertinent travel warnings provided by Government of Canada Travel Advice and Advisories (travel.gc.ca)

(b) review the documentation provided by your DISO

(c) take appropriate precautions to avoid potential risk

(d) limit the information stored on any devices to the minimum data necessary

During travel

(a) avoid the use of untrusted devices (such as foreign host equipment or kiosks)

(b) do not connect to untrusted networks (coffee shops, hotel WIFI, etc.)

(c) if you must connect to the GNB information and resources using an untrusted network, utilize a private location and a secure communication channel (such as VPN)

(d) report all problems or issues to the ITSP as they occur

Upon return

(a) submit devices to the ITSP for forensic analysis (if required)

(b) complete travel return questionnaire and/or attend a travel debriefing session

4.03 IT SDO (e.g., SNB) is responsible to:

Before travel

(a) assess the level of cyber security required for the destination region at the time of travel

(b) properly configure mobile devices prior to departure (may include the issuing temporary replacement devices with a custom setup for use during the trip. The ITSP may also assign temporary user accounts and other credentials to employees as applicable).

(c) ensure encryption of all data stored on travel devices, subject to data encryption laws that may exist at the destination.

During travel

(a) provide technical support for IT issues or problems as reported by travellers

(b) as appropriate for high risk destinations, monitor network, file, and device activity from remotely logged in devices

(c) remote wipe all data on GNB mobile devices that are reported lost by an employee.

Upon return

(a) provide forensic analysis of GNB provided devices (if required)

(b) collect travel return questionnaires and/or conduct a travel debriefing sessions.

4.04 GNB Managed Mobile Devices

- All GNB managed devices containing personal information are subject to GNB support requirements
- All GNB managed devices are subject to ITSP retrieval (seizure) without notice
- Any personal data on GNB managed devices could be subject to technical review or secure wipe without prior employee consultation
- GNB recommends that personally owned mobile devices are never included in business travel
- The use of non-GNB devices to access GNB information during travel,

such as through Exchange, is not acceptable

4.05 Contacts

For IT support questions contact the ITSP.

For questions on personal safety or legal requirements contact the Department of Public Safety, Office of the Provincial Security Advisor.

For general advice and support, contact your DISO. When your DISO is unavailable or unknown, contact Finance and Treasury Board, Chief Information Security Office.

5 DEFINITIONS

- **DISO** – Departmental Information Security Officer
- **Encryption** - encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot
- **Computer Forensics** - is a branch of digital forensic science pertaining to evidence found in computers and digital storage media
- **Information Technology Service Provider** (ITSP) is an organization that provides services for accessing, using, or participating in the GNB Network
- **Secure Wipe** – securely erasing any data on computer or digital device
- **Virtual Private Network** (VPN) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

6 RELATED DIRECTIVES