Office of the Chief Information Officer

Directive

Mobile Devices for Government Employees

Governance

Authority:	Treasury Board
Audience:	All Government departments and public bodies supported by the OCIO.
Compliance Level:	Mandatory
Issuing Public Body:	Office of the Chief Information Officer Infrastructure & Security Branch Information Protection Division
Original Issue Date:	2015-07-23
Date Last Reviewed:	2023-07-30
OCIO Reference:	DOC00363/2015
Version Number:	4.0

Notice:

The Office of the Chief Information Officer (OCIO) is mindful of creating and delivering accessible materials, in line with the Government of Newfoundland and Labrador's Accessible Communications Policy. New materials created by OCIO align with policy requirements and modifications to existing materials will occur as part of the standard review cycle.

This document is available in alternate format. Please contact OCIO@gov.nl.ca.

Forward questions and/or comments related to this document to OCIOInfoProtection@gov.nl.ca.

Table of Contents

1.0 Overview 4
2.0 Purpose 5
3.0 Definitions and Acronyms 6
4.0 Statements 8
5.0 Monitoring of the Network and IT Assets 9
6.0 Roles and Responsibilities 10
7.0 Compliance and Enforcement 11
8.0 Supporting Materials and Version History 12

1.0 Overview

Mobile devices such as laptops, smartphones and tablets are increasingly used within the workplace to provide employees with convenient and flexible access to government information for work purposes. However, due to their portable nature, ability to store large amounts of data and interconnectivity with the Internet, mobile devices in the workplace can increase the risk to government information if they are not managed and secured appropriately.

2.0 Purpose

The purpose of this Directive is to ensure appropriate controls are in place regarding Government-approved mobile devices that have capabilities of connecting to the Government Network (hereafter referred to as 'the Network') and to protect government information that can be accessed and/or used by these mobile devices. The requirements in this Directive are mandatory for all Government departments and public bodies supported by the Office of the Chief Information Officer (OCIO) to follow.

3.0 Definitions and Acronyms

A complete listing of terms are located on the OCIO website - Information Management and Protection (IM&P) Glossary of Terms.

Employee – In the context of this Directive, 'Employee' refers to employees of departments and public bodies supported by the OCIO; it does not include contractors, external consultants, partners, vendors or other third parties entrusted to access or use the Network on behalf of the Government of Newfoundland and Labrador.

Government – In the context of this Directive, 'Government' refers to departments and public bodies supported by the OCIO.

IT Assets – Technology components of an organization such as computers, mobile devices, software, hardware, applications, electronic storage devices, servers, operating systems, and shared drives that have value to the organization.

Mobile Device – A portable computing and communications device with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices) (Source: NISTSP 800-53).

Network – A series of computers and other technology devices that facilitates communications and allows for the sharing of information and resources across an organization, including both wired and wireless technologies.

Smartphone – An 'all in one' mobile phone (e.g., Blackberry, iPhone, etc.) with an underlying operating system that runs applications and software to provide advanced functionality, similar to a computer (e.g., Internet access, email, videos, music, photos, document editing, etc.).

Unmanaged Mobile Device – A government-issued mobile device that is not managed or supported by the OCIO or approved to be attached to the Network (e.g., a smartphone that is not managed by the OCIO's mobile device management solution and is used for cellular services, texting and taking pictures).

The table below includes common abbreviations used by OCIO as well as acronyms found within this document.

Abbreviation	Description
IM	Information Management
IM&P	Information Management and Protection
IP	Information Protection
IT	Information Technology
Network	Government Network
OCIO	Office of the Chief Information Officer

4.0 Statements

1. Employees must only use Government-approved and OCIO[1] managed mobile devices on the Network (e.g., devices procured through the OCIO or a Government master standing offer).

2. Employees must not use personal mobile devices on the Network, as they are not Government-approved devices.

3. In certain instances, departments may procure government owned mobile devices that are not managed by the OCIO. Employees must not connect these Unmanaged Mobile Devices directly to the Network.[2]

4. Employees must only connect an Unmanaged Mobile Device to IT Assets (e.g., laptops, desktops, etc.) that have connectivity to the Network for the purpose of downloading government information (e.g., a smartphone that is not managed by the OCIO's mobile device management solution can be connected to a government IT Asset for the purpose of downloading pictures needed for legitimate government business).

5. Employees must immediately notify the IT Service Desk (servicedesk@gov.nl.ca or 709-729-HELP) if they know of or suspect potential harm to a Government-approved mobile device (e.g., compromised, loss or theft).[3]

6. Employees must return any Government-issued mobile devices to a manager or direct supervisor upon departure from the employ of Government.[3]

7. Employees must adhere to policies and direction from the Office of the Comptroller General in the acquisition and general use of Government-issued mobile devices.[4]

[1] Only the OCIO can approve which mobile devices are issued for use on the Government Network
[2] Connection to personal Wi-Fi networks and/or government "Guest" Wi-Fi access will be permitted
[3] As stated in OCIO's Acceptable Use Directive
[4] https://www.intranet.gov.nl.ca/files/mobile_devices_policy.pdf

5.0 Monitoring of the Network and IT Assets

The Network, its components and all Government IT assets are the property of the Employer and not the property of the Employee. The Employer can add, remove, update and/or block any content, technical or otherwise, and view all Government records (as well as any other records which may be generated, stored on or handled by Government-issued assets), if that action is deemed necessary for the maintenance or security of the Network, or if inappropriate use is suspected. The Employer maintains the right to monitor the Network, its components and all Government IT assets for the purposes of maintenance, repair and management; to ensure continuity of service; to improve business processes and productivity; to meet its legal requirement to produce information; and to prevent misconduct and ensure compliance with the law. The Employer may forward IT assets and/or information to law enforcement agencies when deemed necessary. Employees should be aware these assets, equipment and resources are monitored and will be searched where necessary for the maintenance or security of the Network and government's overall IT environment, or if inappropriate use is suspected, by those authorized to do so on behalf of the Employer or law enforcement agencies. [5]

[5] As stated in OCIO's Acceptable Use Directive

6.0 Roles and Responsibilities

Office of the Chief Information Officer (OCIO)

- Develop, implement and maintain this Directive
- Oversee education and awareness of this Directive across Government
- Monitor and manage the Network and Government IT assets, as required
- Approve what mobile devices are issued for use on the Government Network

Employees

- Be aware of the responsibilities as outlined in this Directive
- Be aware of the requirements for Information Management and Protection
- Adhere to this Directive and any related legislation, policies, directives or standards

Deputy Ministers (or Equivalent)

- Enforce this Directive across their Department or Public Body

Office of the Comptroller General

- Develop, implement and maintain policies on the acquisition and general use of mobile devices

7.0 Compliance and Enforcement

Mandatory Compliance

Adherence to this Directive is mandatory for all employees.

Enforcement

Enforcement of this Directive is the responsibility of the Deputy Minister or equivalent of each department or public body, as per the Management of Information Act, and the Information Management and Protection Policy as approved by Treasury Board, under which it is issued. Where necessary, enforcement will be undertaken by the OCIO in accordance with requirements to secure the Government Network and Government-issued and owned IT assets.

Penalty for failure to comply

Willful non-compliance with this Directive, including contravention through negligence, may result in disciplinary action by the Employer, up to and including termination of employment, in accordance with Government's human resource policies.

8.0 Supporting Materials and Version History

Supporting Materials

Below is a listing of supporting materials hyperlinked to the published location.

Management of Information Act
https://www.assembly.nl.ca/Legislation/sr/statutes/m01-01.htm

Information Management and Protection Policy
https://www.gov.nl.ca/exec/ocio/im/policy-instruments/im-ip-policy/

OCIO Acceptable Use of the Government Network and IT Assets Directive
https://www.ocio.gov.nl.ca/ocio/im/employees/asset_use.html

HR Equipment and Resource Usage Policy
https://www.gov.nl.ca/exec/tbs/working-with-us/equipment-and-resources/

General Policies for Mobile Devices
https://www.intranet.gov.nl.ca/files/mobile_devices_policy.pdf

HR Policies
https://www.gov.nl.ca/exec/tbs/working-with-us/alpha-policies/

Version History

The following table highlights the version history of this document including date issued and version number.

Date (yyyy-mm-dd)	Version
2015-07-23	1.0
2018-05-04	2.0
2018-10-12	2.1
2018-12-13	3.0
2023-07-30	4.0