# Directive – Mobile Devices for Government Employees

**Directive (Definition):** Information Protection and Security (IP&S) directives derive from the Information Management and Protection Policy, TBM 2009-335 approved by Treasury Board on November 19, 2009. IP&S directives are mandatory for users to follow. Directives are supported by standards and guidelines, where applicable.

| Issuing Branch                  | Corporate and Information Management Services (CIMS) Branch  
|                                | Information Protection Division |
| Target Audience                | All Government departments and public bodies supported by the OCIO |
| Approval Date                  | July 23, 2015 |
| Effective Date                 | July 23, 2015 |
| Review Period                  | Every 3 Years |
| Related Standards              | |
| Related Guidelines             | |

## Approval and Sign Off

<table>
<thead>
<tr>
<th>OCIO Senior Leadership Team (SLT)</th>
<th>Approver of IP&amp;S Directives</th>
</tr>
</thead>
<tbody>
<tr>
<td>OCIO Security Council</td>
<td>Approver of IP&amp;S Standards and Guidelines</td>
</tr>
</tbody>
</table>

**Version 1.0**
# Table of Contents

1. Overview ................................................................................................................................ 3  
2. Purpose and Scope ................................................................................................................ 3  
3. Directive Statements ............................................................................................................. 3  
4. Monitoring of the Network and IT Assets ............................................................................. 3  
5. Roles and Responsibilities ..................................................................................................... 4  
6. Definitions and Acronyms ...................................................................................................... 4  
7. Compliance and Enforcement ............................................................................................... 5  
8. Directive Monitoring and Review .......................................................................................... 5  
9. References ............................................................................................................................. 5  
10. Revision History ................................................................................................................... 5
MOBILE DEVICES FOR GOVERNMENT EMPLOYEES

DIRECTIVE

1. 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. Purpose and Scope
The purpose of this Directive is to maintain control of mobile devices used on the Government Network (hereafter referred to as ‘the Network’) and protect government information that is 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. Directive Statements
1. Employees must only use Government-issued\(^1\) 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. 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-issued mobile device (e.g., loss or theft).\(^2\)
4. Employees must return any Government-issued mobile devices to a manager or direct supervisor upon departure\(^3\) from the employ of Government.
5. 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.\(^4\)

4. 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 have no reasonable expectation of privacy as these assets, equipment and resources will be monitored and/or searched, where necessary, by those authorized to do so on behalf of the Employer or law enforcement agencies.\(^2\)

---
\(^1\) Only the OCIO can approve what mobile devices are issued for use on the Government Network.
\(^2\) As stated in OCIO’s Acceptable Use Directive
\(^3\) See Managing Departmental Information through The Employment Cycle Guideline
5. 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

Government Purchasing Agency
- Maintain Government’s master standing offer(s) for mobile devices

6. Definitions and Acronyms

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.

Information Protection (IP) – Information protection is an area of practice focused on the protection of information from inappropriate access or use, using a variety of means as required; including, but not limited to, policy and standards; physical and electronic security measures; and compliance monitoring and reporting. Information Protection represents the point at which the management of information converges with security policy and measures. In the Government of Newfoundland and Labrador, public bodies are required to protect information as part of their accountability under Section 6 of the Management of Information Act SNL2005 c.M-1.01.

Information Protection and Security Program – The comprehensive, organized collection of documented policies, directives, standards, guidelines and processes that are used to continuously deliver information protection and security across the OCIO (Source: Deloitte). This program is managed by the CIMS Branch and is focused on governance, policy and standards; planning and strategy; education and awareness; information risk management; monitoring and compliance; and executive incident response.

Information Protection and Security Policy Framework – Outlines the roles, responsibilities and processes for Information Security policies, directives, standards and guidelines within the OCIO. It also provides the overall model and the supporting method and responsibilities for making the OCIO policies, directives, standards and guidelines a vital element in the overall Information Security Program. The framework depends upon communication and coordination between the various stakeholder roles and responsibilities to ensure that overall risk is well managed.
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) 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.

7. 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. Directive Monitoring and Review
The OCIO is responsible for monitoring and reviewing the content of this Directive. For clarification of this Directive, contact the IT Service Desk at servicedesk@gov.nl.ca or 709-729-HELP.

9. References
Management of Information Act – http://assembly.nl.ca/Legislation/sr/statutes/m01-01.htm


HR Equipment and Resource Usage Policy http://www.exec.gov.nl.ca/exec/hrs/working_with_us/equipment_and_resources.html


HR Policies – http://www.exec.gov.nl.ca/exec/hrs/working_with_us/alpha_policies.html

10. Revision History
July 23, 2015