Office of the Chief Information Officer

Directive

Acceptable Use of the Government Network and/or Information Technology Assets

Governance

Authority:	Treasury Board
Audience:	All staff, contractors, consultants, partners, students, temporary workers, volunteers, vendors, agents, third parties and other persons entrusted to access or use the Government Network and/or IT assets on behalf of the Employer.
Compliance Level:	Mandatory
Issuing Public Body:	Office of the Chief Information Officer Operations & Security Branch Information Protection Division
Original Issue Date:	2013-01-09
Date Last Reviewed:	2022-08-17
OCIO Reference:	DOC00982/2013
Version Number:	3.0

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 10
6.0 Roles and Responsibilities 11
7.0 Compliance and Enforcement 12
8.0 Supporting Materials and Version History 13

1.0 Overview

Access to and use of Government of Newfoundland and Labrador (hereafter referred to as 'Government' or 'the Employer') Information Technology (IT) resources and assets is provided for the sole purpose of conducting Government business and performing work-related activities. It is critical that the Government Network (hereafter referred to as 'the Network') and Government IT assets are protected from unauthorized or inappropriate access or use. Inappropriate access or use of the Network and/or Government IT assets, either knowingly or unknowingly, exposes the Employer to risks that may compromise the protection, security and performance of its information, IT systems and services.

The Network, its components and all Government IT assets are the property of the Employer and not the property of the employee. As such, 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.

2.0 Purpose

The purpose of this Directive is to clearly identify acceptable use of the Network and any Government IT assets, including but not limited to computers; mobile devices such as laptops, smartphones and tablets; applications; software; electronic storage devices; servers; printers; and shared drives. This Directive applies to IT assets owned by the Government or devices approved for use on the Network.

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' includes staff, contractors, consultants, partners, students, temporary workers, volunteers, vendors, agents, third parties and other persons entrusted to access or use the Network and/or IT assets on behalf of the Employer.

Information Protection (IP) – 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. IP 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.

IT Assets – Technology components of an organization such as computers, mobile devices, software, hardware, applications, electronic storage devices, servers, printers 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.

Phishing – Tricking individuals into disclosing sensitive personal information through deceptive computer-based means (Source: NIST SP 800-83). Phishing is a type of fraud that uses deceptive e-mails, websites and/or text messages to gather personal, financial and confidential information for fraudulent purposes and/or unauthorized access.

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.).

Software – Application and system programs that provide instructions and directions to computers and other technology devices.

SPAM – Electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages (Source: NIST CNSSI-4009).

Tablet – A wireless, portable, lightweight computer with a touchscreen interface (e.g., iPad).

Virus – A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk (Source: NIST CNSSI-4009).

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

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

4.0 Statements

1. Employees must securely manage and protect any Government IT assets in their use;

2. Employees must not use the Network or Government IT assets for illegal or criminal purposes or to contravene legislation, policies, directives or standards;

3. Employees must not initiate or participate in any activity that negatively impacts the Network's security or performance;

4. Employees must not gain or attempt to gain unauthorized access to, or circumvent the security controls of, the Network or Government IT assets;

5. Employees must not spread or attempt to spread viruses, SPAM or other malicious content with intent to cause harm to the Network or Government IT assets;

6. Employees must take reasonable precautions to prevent the introduction of viruses, SPAM or other malicious content into or on the Network or Government IT assets;

7. Employees must only use Government-approved and OCIO managed mobile devices on the Network;

8. Employees must only install licensed software on Government IT assets;

9. Employees must only install Government-approved hardware on the Network;

10. Employees must securely manage and protect the usernames and passwords they use on the Network or Government IT assets;

11. Employees must not use the Network or Government IT assets for personal use that interferes with their performance of work-related duties;

12. Employees must not use Network file shares for non-Government purposes;

13. Employees must not use the Network or Government IT assets for personal gain or for any unauthorized commercial purposes;

14. Employees must immediately notify the OCIO IT Service Desk (servicedesk@gov.nl.ca or 709-729-HELP) if they know of or suspect potential harm to the Network or any Government IT assets (e.g., stolen laptop, viruses, SPAM, phishing, compromised user credentials);

15. Employees must return any Government IT assets to a manager or direct supervisor upon departure from the Government;

16. Departments must notify the OCIO IT Service Desk in a timely manner of departing employees (e.g., due to retirement, transfer, dismissal, leave of absence, etc.); and

17. The Employer and Employees must be aware of any legislation, policies, directives, standards and guidelines related to the management, protection and security of Government information. Refer to Section 8 of this Directive, the OCIO's Information Management and Protection website and employees should engage the Director responsible for information management within their department.

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.

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 mobile devices and hardware that can connect to and/or be used on the 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

Departments

- Notify the OCIO IT Service Desk of departing employees

Deputy Ministers (or Equivalent)

- Enforce this Directive across their Department or Public Body

7.0 Compliance and Enforcement

Mandatory compliance

OCIO directives are mandatory for individuals to follow and dictate uniform ways of operating.

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, or contravention through negligence, may result in disciplinary action, up to and including termination of employment/contract or other disciplinary action as per the policies and procedures established by Treasury Board and contractual agreements. Human Resource Policies can be accessed through the following link:
https://www.gov.nl.ca/exec/tbs/working-with-us/policies/#4d

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/

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

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

Directive – Mobile Devices for Government Employees
https://www.gov.nl.ca/exec/ocio/files/publications-policies-directive-mobile-devices-for-government-employees.pdf

FYI – Information Protection in the Workplace – Tops Tips for Protecting Government Information
https://www.gov.nl.ca/exec/ocio/files/FYI-Information-Protection-in-the-Workplace.pdf

FYI - Phishing – Don't Get Hooked
https://www.gov.nl.ca/exec/ocio/files/im-employees-pdf-phishing.pdf

OCIO's Information Management and Protection website
https://www.gov.nl.ca/exec/ocio/im/

Version History

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

Date (yyyy-mm-dd)	Version
2013-01-09	1.0
2015-01-31	2 Year Review
2018-12-17	2.0
2021-03-05	2.1
2022-08-17	3.0