Newfoundland Labrador

Office of the Chief Information Officer

FAQs

Acceptable Use of the Government Network and/or IT Assets

Frequently Asked Questions (FAQs)

1. What is the OCIO's Acceptable Use Directive?

The Office of the Chief Information Officer's (OCIO) 'Acceptable Use Directive' provides a list of activities and actions that Employees must follow in order to maintain the security and performance of the Government Network and Government's IT assets. This Directive gives OCIO the authority to respond accordingly to threats that may impact the security and performance of the Government Network and/or IT assets.

The focus of this Directive is network security and performance. For information on acceptable Internet usage, read the 'Equipment and Resources Usage Policy' in the Human Resources Policy Manual - https://www.gov.nl.ca/exec/tbs/policies/miscellaneous/equipment-and-resources/.

2. Does this Directive apply to me?

The OCIO's Acceptable Use Directive applies to all Government departments and public bodies supported by the OCIO; it is mandatory for all Employees to follow.

Employees, in this context, applies to 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.

3. Why do I need to protect the Government Network and IT Assets?

Failure to properly protect and maintain the performance of the Government Network and IT assets may impact Government's ability to deliver its services to citizens, employees and businesses by compromising the availability and functionality of Government's electronic systems.

Failure to protect the security of the Government Network and IT assets could also result in a breach of Government, citizen and/or business information. As 'Information Protection is Everyone's Responsibility', all employees have an obligation to protect the Government Network and any IT assets in their use.

4. How do I protect the Government Network and IT Assets?

Protecting the Government Network and IT assets is the responsibility of all employees; whether at work or away from the office, you can do your part to protect the Government Network and IT assets by following the guidance and advice available on OCIO's website - https://www.ocio.gov.nl.ca/.

In particular, OCIO points you to the following:

- CyberSafeNL https://www.cybersafenl.ca/

Employees are also strongly encouraged to complete the online Cyber Security Awareness e-Learning Module, which is accessible through Government's Learning Management System, PS Access. This short and simple e-learning module helps employees understand the important role they play in recognizing cyber threats and taking action to prevent cyber-attacks to the Government Network and its IT devices. Employees can access the course through www.psaccess.ca. All employees should complete this training to ensure they are fully informed of their responsibilities to protect against cyber threats in the workplace.

5. Does the OCIO have the right to monitor and access my computer?

Yes. The Network, its components and all Government IT assets are the property of the Employer and not the property of the Employee. 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.

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 may forward IT assets and/or information to law enforcement agencies when deemed necessary.

If the OCIO is asked by a Department to provide an Employee's usage or monitoring history (e.g., list of Internet sites visited) access to an Employee's records (e.g., email, 'p' drive), the OCIO will provide this information to the Department. The OCIO will also provide access to records for the purpose of responding to an ATIPP or legal discovery request, at the request of a Department.

6. What are 'approved' mobile devices?

Only the OCIO can determine (i.e. approve) what mobile devices can connect to and/or be used on the Government Network. At this time, employees are not allowed to use personal mobile devices (laptops, tablets or smartphones) on the Government Network.

For more information on network use of mobile devices, see the OCIO's Mobile Devices Directive for Government Employees - https://www.gov.nl.ca/exec/ocio/files/Directive-Mobile-Devices-for-Government-Employees.pdf.

7. What type of activity is considered 'illegal or criminal'?

Please read the 'Equipment and Resources Usage Policy' in the Human Resources Policy Manual - https://www.gov.nl.ca/exec/tbs/policies/miscellaneous/equipment-and-resources/.

8. What type of activity negatively impacts network performance?

The Government Network serves as the connection hub for all of Government's electronic systems; it is the mechanism that allows systems and Employees to communicate with each other. Some activities, however, use up a significant amount of the Government Network's resources and slow down its ability to run its systems properly.

Activities that can negatively impact network performance include but are not limited to streaming video and voice (e.g., YouTube, radio stations), online gaming and the downloading large files such as movies, MP3's and other audio/video files.

If the OCIO determines than an Employee's activity is negatively impacting the performance of the Government Network, the OCIO has the authority to take steps to prevent or stop that activity.

9. How can I protect against SPAM, viruses and other malicious content?

As you incorporate email and the Internet into your daily work activities, you increase your exposure to Internet-based threats such as SPAM, viruses, phishing (see Recognizing Phishing Attacks - https://www.cybersafenl.ca/recognizing-phishing-attacks/ and other forms of malicious content, known as 'cybercrime'. As an employee, you have a responsibility to do your part to reduce the threat of cyber-attacks.

For more information on Cyber Security, visit the Cyber Security Office website at https://www.gov.nl.ca/cso/.

To ensure cyber threats are limited, follow these steps:

1. Never disclose your government-issued username and password.
2. Never click on links or attachments in e-mails from unknown sources.
3. Never use your government-issued e-mail address for personal use.
4. Do not answer suspicious emails even if they appear legitimate.
5. Suspicious emails often appear to be from a recognized organization or client. Contact the legitimate organization or client through another means of communication (e.g., by phone; do not use the contact information in the email you received but rather from previously established contact list) and ask if they sent such an email. If uncertain, speak to your supervisor.
6. Avoid storing files locally on your government desktop or laptop. You should always store files on a network drive where they can be backed up. If you must store files temporarily on a local hard drive always ensure you are backing up the data on a

regular basis. Otherwise, if your computer was compromised, you would not have a copy of your file/data and it is highly unlikely the OCIO would be able to recover any deleted/encrypted files.

10. What is 'licensed' software?

Licensed software, which may be free of charge or purchased, requires the user/purchaser to accept an 'end user agreement' stating conditions for using the software. For example, software purchased or obtained from the 'Apple Store' and 'Blackberry App World' is licensed.

Before you acquire licensed software, OCIO cautions you to:

- Avoid use of software that requires or allows for auto-syncing with cloud services.
- Only obtain software that is needed to perform your work-related duties.
- Verify that the software is from a trusted source.
- Check that the software has a valid digital signature.
- Consult your departmental Director responsible for Information Management to engage the OCIO for a software review prior to purchase.

If the OCIO determines that installed licensed software is negatively impacting the security or performance of the Government Network, the OCIO has the authority to secure, update and/or remove the licensed software.

11. What is 'Government-approved' hardware?

Only the OCIO can determine (i.e. approve) what hardware can connect to and/or be used on the Government Network. Hardware is the physical equipment that makes up a computer system, including but not limited to laptops, desktop computers, external hard drives and peripheral devices such as monitors, printers, scanners and other multi-function devices. You are only allowed to install hardware on the Government Network that has been approved for use by the OCIO. For more information on Government-approved hardware, contact the OCIO IT Service Desk at servicedesk@gov.nl.ca or 709-729-HELP (4357).

12. Can I store personal photos and documents on shared drives?

No. Only Government-related files can be stored on shared drives located on the Government Network. Personal photos, music files and other personal documents cannot be stored on network drives.

The Government Network is to be used for the storage of Government information only. The OCIO backs up the Network on a regular basis, which has time and cost implications for Government. The enterprise network and backup solution should only be used to house and support Government business.

If you must store personal files on your government-issued computer, you should save it to your local drive (i.e. 'C' drive; My Documents, Desktop).

13. Does this Directive apply to personal devices?

No. At this time, employees are not allowed to use personal mobile devices (laptops, tablets or smartphones) on the Government Network. For more information on network use of mobile devices, see the OCIO's Mobile Devices Directive for Government Employees - https://www.gov.nl.ca/exec/ocio/files/Directive-Mobile-Devices-for-Government-Employees.pdf.

If you have been approved to use a personal device for the purpose of doing Government business prior to implementation of this Directive, you are bound by any Terms of Use document that was signed when approval to use the device was granted.

14. Who do I contact if I have questions about the Acceptable Use Directive?

If you have questions about the Acceptable Use Directive or this FAQ, please contact OCIOInfoProtection@gov.nl.ca.

Supporting Materials

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/

Acceptable Use of the Government Network and/or Information Technology Assets Directive
https://www.gov.nl.ca/exec/ocio/im/employees/asset-use/

Equipment and Resource Usage Policy
https://www.gov.nl.ca/exec/tbs/policies/miscellaneous/equipment-and-resources/

OCIO Website
https://www.ocio.gov.nl.ca/

CyberSafeNL
https://www.cybersafenl.ca/

Government's Learning Management System, PS Access
www.psaccess.ca

Directive – Mobile Devices for Government Employees
https://www.gov.nl.ca/exec/ocio/files/Directive-Mobile-Devices-for-Government-Employees.pdf

Recognizing Phishing Attacks
https://www.cybersafenl.ca/recognizing-phishing-attacks/

Cyber Security Office
https://www.gov.nl.ca/cso/

Version History

Date (yyyy-mm-dd)	Version
2013-01-29	1.0
2016-09-22	2 Year Review
2018-12-14	2.0
2021-03-04	2.1
2022-08-17	3.0
2023-03-22	3.1
2025-09-19	3.2