FYI

Information Protection in the Workplace

Top Tips for Protecting Government Information

Overview

Information Protection (IP) 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. 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. All government employees and contractors must manage and protect information in their custody or control.

Best Practices

Cyber Security

- Never disclose a government-issued username or password.
- Never click on links or attachments in emails from unknown sources.
- Never use your government-issued email address for personal use.
- If you receive a suspicious e-mail or text message from a recognized organization or client, contact the legitimate organization or client by another means (e.g., by telephone).

Acceptable Use of the Network and/or IT Assets

- Do not use personal mobile devices on the government network (e.g., smartphones, tablets).
- Only install and use approved software and hardware.

Password Management

- Create unique passwords with strong password complexity (e.g., 8 characters, upper/lower case, #'s and letters).
- Immediately report stolen or compromised passwords to OCIO's IT Service Desk at (709) 729-4357 (HELP).

Safe Email Practices

- Do not use personal email accounts to conduct government business. Review and adhere to the Directive – Use of Non-Government Email Accounts for Work Purposes.
- Limit use of web-based email services (e.g., Gmail, Hotmail, Yahoo Mail).

Safe Business Practices

- Do not save government information on a local drive (e.g., C drive, My Documents folder, Desktop).
- Always lock your workstation when you leave your desk by using Control-Alt-Delete.
- Employees must only access information they require to perform duties associated with their job.
- Employees may have access to information that cannot be shared with family, friends and even other government employees. Do not be afraid to ask questions or delay a response to an inquiry to verify whether it is appropriate to share information with a client, business partner or another government employee.
- Avoid "elevator" conversations; business discussions overheard in public places may result in information being disclosed inappropriately or being interpreted out of context.
- Be discreet if you must view government information in public places.
- When accessing government information, over a wireless network, only do so through a secured VPN connection using a government-issued laptop or tablet.
- Book meeting rooms to discuss sensitive matters and ensure distributed copies of records are retrieved and returned to the office for secure disposal. Erase content from white boards and remove pages from flip charts before leaving a meeting room.
- Implement a "clean desk" practice to ensure that visitors do not inadvertently access information they should not see.
- If you have visitors to your work area for meetings, ensure that you follow your building security procedures to properly register their visit.
- Notify your manager immediately if you require additional information about implementing safe business practices or if you suspect that information has been inappropriately accessed.

Safe Transferring of Information Practices

- Always double check that you do not leave information behind when exiting a car, room etc.
- Don't carry loose documents or open file folders.

- Secure Management File Transfer (SMFT)
    - SMFT is sanctioned for transferring secret, confidential or sensitive government information.
    - The Managed File Transfer Request Form would need to be completed if you currently do not have a SMFT account.
    - The OCIO recommends external users log in once a month to keep their account active, as accounts that are not used for a period of 90 days will expire.
    - SMFT has a global retention period of 7-days and cannot be tailored per individual departmental needs. If the file is not picked up after 7 days, it is deleted and would need to be resent.
    - SMFT employs a one-time password for all users. The user community is expected to agree to use all the security features employed by SMFT.
    - SMFT Accounts are created within 24 hours. Once account is setup, you will be prompted to log in (email address, password you use to login to your computer, type in one time code). Once logged in, users will encounter an email "like" window.
    - The recipient of the file transfer will receive an email with a link. Once the link is clicked, the user will be stepped through an account process automatically (e.g., create password, sent one time passcode, etc.).

- Faxing Information
    - Check fax numbers carefully or use programmed numbers for frequently faxed locations.
    - Notify the recipient that the fax is being sent and verify with the recipient that the fax has been received.

- USB Flash Drives
    - Do not store confidential government information on USB flash drives that are not encrypted.
    - Do not purchase or otherwise distribute USB flash drives for promotional purposes.

Cloud-Based Software and Services (e.g., Dropbox, Box.com, One Drive, Adobe Acrobat, Adobe Reader)

- Disable automated file transfer of synchronization features when using cloud-based software or services.
- Do not use cloud-based software or services to share or store personal or confidential information.

Cyber Security is **EVERYONE's** responsibility. For more information, contact OCIOInfoProtection@gov.nl.ca.

Supporting Materials

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

Cyber Security Awareness
https://www.gov.nl.ca/exec/ocio/security/cybersecurity/

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

Standard - Password Management
https://www.gov.nl.ca/exec/ocio/files/publications-policies-standard-password-management.pdf

Directive – Use of Non-Government Email Accounts for Work Purposes
https://www.gov.nl.ca/exec/ocio/im/policy-instruments/email-management/

FYI – Information Protection – USB Drives – What You Should Know
https://www.ocio.gov.nl.ca/ocio/im/employees/pdf/FYI_Information_Protection-USB_Drives.PDF

Managed File Transfer Request Form
https://ociohelp.psnl.ca/files/Managed-File-Transfer-Request-Form-UPDATE.pdf

FYI - Cloud-Based Storage Services
https://www.gov.nl.ca/exec/ocio/files/im-employees-pdf-cloud-based-storage-services.pdf

Version History

Date (yyyy mm dd)	Reference
2016-09-30	1.0
2022-10-01	2.0