Make Time @Work for IM!

Employees are responsible for managing and protecting the government information they use to do their jobs. The Office of the Chief Information Officer (OCIO) is asking you to take a minute at the beginning of your meeting to review this Information Management (IM) best practice. Remember, small changes in the way you work can make a big impact on our compliance with government's IM requirements.

Portable Storage Devices

There have been many reports in Canada where personal or confidential information has been lost or misplaced on a portable storage device. Portable storage devices including flash drives, jump drives, memory sticks, USBs, CDs, etc., can store a large amount of data. Because they are small and portable, they may be easily lost.

- Is storage on a Portable storage device necessary? Information that is stored on the government network is secure because a user must have a network account and permission to access it. The OCIO also backs up the data stored on the network meaning there is no need to make a personal copy for security purposes
- If you use a portable storage device, use an encrypted device that requires user authentication to access the data stored within
- Use portable storage devices as temporary storage for files that you must access when the government network is unavailable. On your return to the office, transfer files back on to the network and delete them from the portable storage device
- Follow up with your manager on remote access options if your role requires that you access personal or confidential information offsite on a frequent basis
- Report a lost or stolen portable storage device to the OCIO IT Service Desk 729-help

To learn more about IM Best Practices contact your departmental IM division or visit the OCIO website: www.ocio.gov.nl.ca

For more information visit **www.ocio.gov.nl.ca**
or email us at IM@GOV.NL.CA

Newfoundland Labrador