National Defence / Défense nationale

VICE CHIEF OF THE DEFENCE STAFF

DIRECTOR GENERAL DEFENCE SECURITY

VCDS – VCEMD

Working remotely from home and alternative work locations

Security of Information

Working remotely brings security challenges. From juggling work with kids at home, learning how to use new IT programs/equipment and even managing work paper files. **We must stay VIGILANT.**
The compromising of information of the Department of National Defence (DND) and the Canadian Armed Forces (FAC) could harm the Canada and Allies interests, DND/CAF operational tasks and the safety of personnel.

While you're getting your work-at-home systems set up, here are some tips for protecting DND and CAF information.

TIPS AND TRICKS

- **Treat removable media the same way as you would treat sensitive physical files**
  Sensitive information (such as paper copies, CD's, DVDs, USB keys or other media) must be stored appropriately when not in use.
- **Use the DWAN network for the processing of information**
  Up to PROTECTED A and PROTECTED B when using the DND/CAF Public Key Infrastructure (PKI) card.
- **Know and follow DND/CAF policies for the secure access, use, disclosure, modification, storage, transmission, disposal or destruction of information, to prevent the compromise of information through accident or neglect**
- **Identify your Unit Security Supervisor (USS) for all your security questions**
- **Identify your Information Systems Security Officer (ISSO) for all your IT security questions**
- **Let your supervisor/manager, USS and ISSO know if security rules aren't being followed or can't be followed**
- **Always follow secure handling requirements and proper security marking on information**
  This maintains the security and confidentiality of information held by DND/CAF.

WHAT NOT TO DO

- **Laptops can be used to process classified/protected information (if they are accredited and approved for such use). When not in use, they have to be secured according to the requirements for the classified/protected information being processed**
  It is prohibited to connect a laptop that processes classified/protected information higher than Protected B to the DWAN and to the Internet.
- **Sensitive information may not be removed from the applicable secure zone without justification and without getting permission from the approved authority**
- **Do not remove laptops used for protected or classified information from the office**
  If such laptops need to be transported, written permission must be obtained from the approved authority.
- **Do not release any sensitive information to the public and to anyone who does not have a need-to-know or proper security clearance. Also, do not share classified or sensitive information on social media**
  Unclassified information does not automatically mean it can be released to the public or be open to all DND employees and CAF members without a need-to-know. Approved release procedures must be followed.
- **Do not work on sensitive material from home without permission**
- **Do not bring home sensitive or classified documents without getting permission from the approved authority**
  In an office, always use an approved folder and use an approved briefcase or bag for outside.

Immediately report any security incidents to your local **Information System Security Officers (ISSO)** or **Unit Security Supervisor (USS)**

FOR MORE TIPS AND INFORMATION:

NDSOD - Chapter 6 - Security of Information, Security of Information Standards
collaboration-admpa.forces.mil.ca/sites/DI/SafetySecurity/vcds-ndsod-s06.pdf

A-SJ-007-000/DA-094
OPI: DGDS BPR: DGDS
2020/09

SECURITY NEVER TAKES A BREAK. | **VIGILANCE!**

Canada