National Defence / Défense nationale

VICE CHIEF OF THE DEFENCE STAFF

DIRECTOR GENERAL DEFENCE SECURITY

VCDS – VCEMD

Working remotely from home and alternative work locations

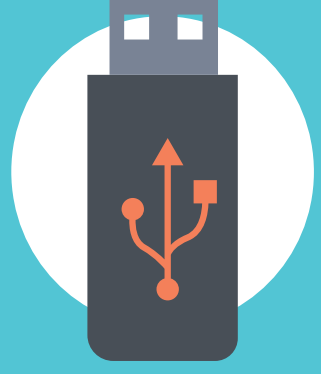
DWAN T-DVPNI laptops and devices

Many DND employees and CAF members are adjusting to the "new normal" of working remotely. In order to ensure successful, safe, and secure remote work, additional measures will need to be taken to protect DND/CAF devices and network and to safeguard its information.

You must be vigilant while using your laptop and devices.

TIPS AND TRICKS

- **Always use the appropriate device for the appropriate network (i.e. DWAN with DWAN T-DVPNI)**
- **Use your laptop exclusively for work and do not let family members or others use it**
  Access to the DWAN is only granted once the user's Reliability Check is confirmed and the user has read and signed the DWAN Access Control and Authorisation Form.
- **Your laptop and devices must not be left unattended when in public view**
  It should be carried by the employee at all the times or be physically secured when not in use. It is recommended that your devices be locked in luggage, stored in a secure lock-up, or locked with a secure cable. Your Public Key Infrastructure (PKI) card should be treated the same as it is a sensitive security item and an essential for connecting to T-DVPNI.
- **Your laptop must not be checked as baggage when travelling by rail, plane or bus**
- **Always follow IT security rules**
- **Only use authorized USB storage/thumb drives, duly registered, labelled, password protected, encrypted, and physically secured**
  USB devices, tablets, laptops or mobile phones must be properly secured at all times. Secured to the appropriate highest level of security classification of the information stored on it.



- **If you forget your DWAN password: a new one will be assigned**
  Before changing a password for a user, an officially appointed ISSO will confirm that the user is a legitimate one.
- **The serial number of your laptop must be recorded by the user**
  That way, in the event of a theft, a full report may be made to the nearest Military Police Unit, to the local ISSO or if it occurred outside of DND/CAF premises, to the nearest local Police Agency.

WHAT NOT TO DO

- **Do not plug a personal USB key or any other private device into your laptop**
  This includes: phones, LTE devices, tablets, printers, fax machines, and cameras. You can only use DND/CAF approved devices.
- **Do not download or attempt to install any unknown software**
  Only a software that is authorized by the service management desk is to be used.
- **The use of private cloud storage services such as Google Drive, DropBox and iCloud to store DND/CAF unclassified documents or information is not permitted**

- **Do not remove laptops used for protected or classified information from the office**
  If such laptops need to be transported out of the office, written permission must be obtained from the approved authority.

Immediately report any security incidents to your local **Information System Security Officers (ISSO)** or **Unit Security Supervisor (USS)** if you suspect you may have been exposed to a virus or malware or if your IT devices have been compromised.

A-SJ-007-000/DA-092
OPI: DGDS BPR: DGDS
2020/09

FOR MORE TIPS AND INFORMATION:

Immediate contact IT security – Local ISSO

National contact – DIM Secur OPS positional mailbox
++DIM Secur OPS@ADM(IM) DIM Secur@Ottawa-Hull

Defence Wide Area Network (DWAN) Information Systems (IS) Security Orders can be consulted

SECURITY NEVER TAKES A BREAK. | VIGILANCE!

Canada