National Defence / Défense nationale

VICE CHIEF OF THE DEFENCE STAFF

DIRECTOR GENERAL DEFENCE SECURITY

## Working remotely from home and alternative work locations

# DEFENCE O365

### WHAT IS O365?

*Also known as The Enterprise Cloud Network (ECN)*

MICROSOFT 365 is a set of Internet-accessible cloud-based applications to support teleworking and collaboration, including:

**Word** **Excel** **One Note** **MS Teams**

and much more

## WHAT IS MICROSOFT TEAMS?

**Microsoft (MS) Teams is a unified communication and collaboration platform you can use on your personal devices** for you and your colleagues while working remotely.

**IT INCLUDES:**

- Workplace chat
- Video conference meetings
- File storage
- Sharing transitory information

**This tool has been approved to storing and processing up to Protected A information. Other public cloud services platforms are not assessed for security and must be used only with approved information.**

## WHY USE IT?

This solution is being deployed to DND/CAF to facilitate working from home during the COVID-19 emergency period. This will reduce the strain on the DWAN T-DVPNI network.

- **Defence O365 can be accessed and used on your personal devices**
- **The products are reputable**
- **It has been security tested**

## EASY TIPS TO ADOPT CYBER SECURITY BEST PRACTICES

✓ **Avoid blending your work and personal environments**
e.g. use separate user accounts for different roles and do not allow anyone else to use your accounts.

✓ **If you use your shared family computer:**
Create a separate and dedicated user account and always lock your sessions with a password when absent.

✓ **Respect the privacy of your teammates**
Ask for their consent before creating accounts for others or inviting teammates to use a service through their personal email addresses.

✓ **You are not permitted to use unauthorized USB devices on Defence systems to move or to store files**

✓ **Use Google Chrome**
It is the recommended web browser.

✓ **Ensure your home computer is up-to-date**
e.g. operating system, web browsers, software, vendor-recommended updates are applied, etc.

✓ **Use up-to-date security software (anti-virus) on your home computer and connected devices**
Set device security software and operating systems to auto-update.

A-SJ-007-000/DA-090
OPI: DGDS BPR: DGDS
2020/09

SECURITY NEVER TAKES A BREAK. | VIGILANCE!

Canada


- ✓ **Secure your network**
  An unsecured network means that anyone with a Wi-Fi device in your coverage area can access your personal Internet connection and your devices.
- ✓ **Ensure that your home Internet router has all vendor software patches installed**
  - ***If you rent your router:*** this may be done automatically by your Internet service provider.
  - ***If you own your own router:*** you will need to verify this yourself. Refer to your router vendor's website for details.
- ✓ **Change the manufacturer's default user names and use strong passwords for your Wi-Fi network and smart devices**
  Don't use anything that could be associated with your name, address or phone number.
- ✓ **Do not fall for phishing emails posing as DND/CAF messages and avoid opening email attachments from unknown sources**
  Official communications will always come from a trusted and secure source.
- ✓ **Only share unclassified information. No sensitive information is permitted:**
  Protected B, Classified, Controlled Goods and International Traffic in Arms Regulations information is not permitted on Defence O365 at this time.

- ✓ **Secure your social media and email accounts**
- ✓ **Install a firewall, and configure it to restrict traffic coming into and leaving your computer**
- ✓ **Be cautious if you notice that your Internet connection is unusually slow or if you can't access to certain sites**
- ✓ **Monitor your virtual community**
  Help to ensure that no sensitive information is uploaded.
- ✓ **Set the camera and microphone to off when not in use**

## ECN RELATED

**DND/CAF information shall not be copied or transferred from ECN environment to personal devices outside the associated Internet browser (Chrome) session or approved Microsoft O365 applications.**

**All content in ECN is subject to disclosure under the Access to Information Act and Privacy Act. All users are responsible for safeguarding information of sensitive nature, such as personal information applying the "Need to Know" principle.**


**Report any security issues to your ISSO, USS, or**
**cloudsecuritymonitoring@jdcp.forces.gc.ca**

For more details on security best practices, please consult **www.getcybersafe.gc.ca**

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