Le travail à distance à domicile et dans les lieux de travail auxiliaires

O365 DE LA DÉFENSE

QU'EST-CE QUE O365 ?

Aussi appelé le Réseau en Nuage de l'Entreprise (RNE)

MICROSOFT 365 est un ensemble d'applications infonuagiques accessibles par Internet facilitant le télétravail et la collaboration. Il contient notamment :

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

et bien plus encore

QU'EST-CE QUE MICROSOFT TEAMS ?

Microsoft (MS) Teams est une plateforme de communication et de collaboration unifiée que vous et vos collègues pouvez utiliser sur vos appareils personnels pour communiquer pendant que vous travaillez à distance.

VOICI QUELQUES FONCTIONS DE TEAMS :

- clavardage en milieu de travail
- rencontres par vidéoconférence
- stockage de fichiers
- échange d'information éphémère

Cet outil a été approuvé pour le stockage et le traitement d'information pouvant aller jusqu'à Protégé A. Les autres plateformes publiques de services infonuagiques n'ont pas fait l'objet d'une évaluation de sécurité. Elles ne doivent donc être utilisées qu'avec de l'information autorisée.

POURQUOI L'UTILISER ?

Le déploiement de cette solution au MDN et dans les FAC est en cours et a pour but de faciliter le télétravail pendant la période d'urgence de la COVID-19. Cela permettra d'éviter de surcharger l'IRPVD-T ayant accès au RED.

- **l'O365 de la Défense est accessible et utilisable sur vos appareils personnels**
- **les produits sont fiables**
- **il a été soumis à des tests de sécurité**

CONSEILS INSPIRÉS DES PRATIQUES EXEMPLAIRES EN MATIÈRE DE CYBERSÉCURITÉ

✓ **Évitez de mêler votre environnement de travail à votre environnement personnel**
c'est-à-dire : servez-vous de comptes distincts pour vos différents rôles et ne permettez à personne d'utiliser vos comptes.

✓ **Si vous utilisez un ordinateur familial auquel d'autres ont accès :**
Créez un compte d'utilisateur dédié et distinct et verrouillez votre session avec un mot de passe lorsque vous vous absentez.

✓ **Respectez la vie privée de vos coéquipiers**
Demandez aux autres de vous donner leur consentement avant de créer des comptes pour eux ou de les inviter en utilisant leur adresse courriel personnelle.

✓ **Il est interdit d'utiliser des appareils USB non autorisés pour déplacer ou stocker des fichiers dans les systèmes de la Défense**

✓ **Utilisez Google Chrome**
Il s'agit du navigateur Web recommandé.

✓ **Assurez-vous que votre ordinateur personnel est à jour**
(système d'exploitation, navigateurs Web, logiciels, mises à jour recommandées par le fabricant logiciel, etc.).

✓ **Servez-vous d'un logiciel de sécurité à jour (antivirus) pour protéger votre ordinateur à domicile et les appareils qui y sont connectés**
Activez la mise à jour automatique des logiciels de sécurité et des systèmes d'exploitation de vos appareils.

A-SJ-007-000/DA-091
OPI: DGSD BPR: DGSD
2020/09

✓ **Sécurisez votre réseau**
Si votre réseau n'est pas sécurisé, toute personne avec un appareil Wi-Fi dans la zone de couverture de votre réseau sans fil peut accéder à votre connexion Internet personnelle et à vos appareils.

✓ **Assurez-vous que tous les correctifs de logiciels diffusés par le fabricant de votre routeur Internet à la maison ont été installés**
- ***Si vous louez votre routeur :*** il est possible que la mise à jour soit faite automatiquement par votre fournisseur de services Internet.
- ***Si vous êtes propriétaire de votre routeur :*** vous devrez vous-même vérifier que les mises à jour ont été installées. Consultez le site Web du fabricant de votre routeur pour en savoir plus à ce sujet.

✓ **Modifiez les noms d'utilisateur par défaut du fabricant et utilisez des mots de passe robustes pour sécuriser votre réseau et vos appareils sans fil**
N'utilisez rien qui pourrait être associé à votre nom, votre adresse ou votre numéro de téléphone.

✓ **Méfiez-vous des courriels d'hameçonnage qui imiteraient les messages du MDN ou des FAC et évitez d'ouvrir les pièces jointes de courriels provenant de sources que vous ne connaissez pas**
Les communications officielles proviennent toujours d'une source fiable et sécurisée.

✓ **Ne partagez que des données non classifiées. L'information de nature sensible ne peut être divulguée :**
l'information Protégé B, des renseignements classifiés et toute information concernant le Règlement sur les marchandises contrôlées et l'International Traffic in Arms Regulations ne peuvent être divulgués sur l'O365 de la Défense à l'heure actuelle.

✓ **Sécurisez vos comptes dans les médias sociaux et vos comptes de courrier électronique**

✓ **Installez un pare-feu et configurez-le pour qu'il limite le trafic entrant et sortant de votre ordinateur**

✓ **Méfiez-vous si vous remarquez que votre connexion Internet est particulièrement lente ou si vous n'arrivez pas à accéder à certains sites**

✓ **Surveillez votre communauté virtuelle**
Veillez à ce qu'aucune information de nature sensible ne soit transmise.

✓ **Éteignez votre caméra et votre microphone lorsque vous ne les utilisez pas**

AU SUJET DU RNE

L'information du Réseau en Nuage de l'Entreprise (RNE) du MDN et des FAC ne doit en aucun cas être copiée ou transmise de l'environnement du RNE à un appareil personnel en dehors de la session du navigateur Internet (Chrome) ou des applications autorisées de Microsoft O365.

Tout le contenu du RNE pourrait devoir être divulgué en vertu de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels. Tous les utilisateurs sont chargés de protéger les renseignements de nature sensible, par exemple les renseignements personnels, en appliquant le principe du besoin de connaître.

Signalez tout incident de sécurité à votre OSSI, à votre SSU ou à l'adresse
cloudsecuritymonitoring@jdcp.forces.gc.ca

Pour en savoir plus sur les pratiques exemplaires en matière de sécurité, consultez le site **www.pensezcybersecurite.gc.ca**

LA SÉCURITÉ NE PREND JAMAIS DE PAUSE. | **VIGILANCE!**