Défense nationale | National Defence

VICE-CHEF D'ÉTAT-MAJOR DE LA DÉFENSE

DIRECTEUR GÉNÉRAL - SÉCURITÉ DE LA DÉFENSE

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

Sécurité de l'information

Le télétravail pose des défis en matière de sécurité. Qu'il s'agisse de concilier le travail et la présence des enfants, d'apprendre à utiliser de nouveaux programmes informatiques et même de gérer les dossiers papier au travail, l'important, c'est de **rester VIGILANT**. La compromission de l'information du ministère de la Défense nationale (MDN) et des Forces armées canadiennes (FAC) pourrait nuire aux intérêts du Canada et des Alliés, aux tâches opérationnelles du MDN et des FAC et à la sécurité du personnel.

Tandis que vous configurez les systèmes vous permettant de travailler à domicile, voici quelques conseils afin de protéger l'information du MDN et des FAC.

TRUCS ET CONSEILS

- **Traitez les supports électroniques amovibles de la même manière que les dossiers papier de nature sensible**
  Les renseignements de nature délicate (sur papier, CD, DVD, clé USB ou un autre support) doivent être entreposés de façon appropriée lorsqu'ils ne sont pas utilisés.
- **Utilisez le RÉD pour traiter les renseignements**
  De niveau PROTÉGÉ A et PROTÉGÉ B lorsque vous utilisez la carte d'infrastructure à clé publique (ICP) autorisée par le MDN et les FAC.
- **Il faut bien connaître et respecter les politiques sur la sécurité entourant l'accès, l'utilisation, la communication, la modification, le stockage, la transmission, l'élimination ou la destruction pour empêcher la compromission d'informations par accident ou par négligence**
- **Identifiez votre surveillant de la sécurité de l'unité (SSU) pour toute question de sécurité**
- **Identifiez votre officier de la sécurité des systèmes d'information (OSSI) pour toute question relative à la sécurité des TI**
- **Prévenez votre superviseur ou gestionnaire, votre SSU et votre OSSI si les règles concernant la sécurité ne sont pas respectées ou s'il est impossible de les suivre**
- **Toujours respecter les exigences de manipulation sécurisée et le bon étiquetage de sécurité sur les informations**
  Ces mesures assurent la sécurité et la protection des informations que détiennent le MDN et les FAC.

CONSEILS JUDICIEUX

- **Les ordinateurs portatifs peuvent être utilisés pour traiter les renseignements classifiés ou protégés (s'ils ont été homologués et autorisés pour ce genre d'utilisation). Lorsqu'ils sont inutilisés, ils doivent être sécurisés conformément aux exigences régissant les renseignements classifiés ou protégés**
  Il est interdit de brancher au RÉD un ordinateur portatif qui traite des renseignements classifiés ou protégés dont le niveau de sécurité est supérieur à Protégé B.
- **Il est interdit de retirer de la zone sécurisée pertinente les renseignements de nature sensible, à moins d'obtenir l'autorisation de l'autorité approbatrice**
- **Ne pas retirer du bureau les ordinateurs portatifs qui servent aux renseignements protégés ou classifiés**
  Si ces ordinateurs portatifs doivent être transportés, il faut obtenir l'autorisation écrite de l'autorité approbatrice.
- **Ne divulguez aucune information sensible au public et aux personnes qui n'ont pas un besoin de connaître ou ne possedant pas une habilitation de sécurité appropriée. De plus, ne partagez pas d'informations classifiées ou sensibles sur les réseaux sociaux**
  Les informations non classifiées ne signifient pas automatiquement qu'elles peuvent être rendues publiques ou ouvertes à tous les employés du MDN et aux membres des FAC sans avoir un besoin de connaître. Les procédures de diffusion approuvées doivent être suivies.
- **Ne travaillez pas sur du contenu de nature sensible à domicile à moins d'avoir obtenu l'autorisation de le faire**
- **Ne rapportez pas de documents classifiés ou de nature sensible à la maison sans obtenir l'autorisation de l'autorité approbatrice**
  Au bureau, utilisez toujours un dossier approuvé et utilisez un porte-document ou un sac approuvé si vous sortez du batiment.

Signalez immédiatement tout incident de sécurité à votre **officier de la sécurité des systèmes d'information (OSSI)** local ou au **surveillant de la sécurité de l'unité (SSU)**

POUR PLUS DE CONSEILS ET INFORMATION :

ODSDN, chapitre 6 : Sécurité de l'information, Normes de sécurité de l'information
collaboration-admpa.forces.mil.ca/sites/DI/SureteSecurite/vcemd-odsdn-c06.pdf

A-SJ-007-000/DA-095
OPI: DGSD BPR: DGSD
2020/09

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

Canada