



RISQUES INTERNES

Certaines menaces à notre sécurité proviennent-elles de l'interne? ▶

Les menaces ne proviennent pas que des espions ou des cybercriminels, elles peuvent venir de toute personne qui est ou a été employée au sein du MDN ou des FAC : un employé, un membre des FAC, un entrepreneur ou un étudiant – toute personne ayant accès à des informations sensibles, des ressources, des personnes ou des installations, qui pourrait nuire à l'organisation. La cause peut être la **malveillance**, l'**imprudence** ou même l'**ignorance**... mais les dommages sont les mêmes.

Cela affecte notre personnel.

Les risques liés à la sécurité peuvent :

- Compromettre des renseignements classifiés ou des systèmes TI
- Mettre en péril les opérations et la sécurité du personnel
- Nuire à la réputation internationale et aux partenariats du Canada
- Causer des pertes financières et opérationnelles

Types de risques internes

Intentionnels ou non

▶ Imprudent

EX: Laisser les systèmes déverrouillés, cliquer sur des liens d'hameçonnage, divulguer trop d'informations en public ou assurer une mauvaise sécurité des opérations (SECOP)

▶ Radicalisé/ idéologique

EX: Promouvoir des opinions extrémistes ou des affiliations contraires aux valeurs du MDN et des FAC

▶ Compromis

EX: Exploité par un tiers : accès détourné au moyen d'un logiciel malveillant, d'une tentative d'hameçonnage ou de coercition

▶ Anciens employés mécontents

EX: Utiliser un accès résiduel ou des connaissances à des fins préjudiciables

▶ Malveillant

EX: Vendre ou divulguer publiquement des renseignements classifiés à des fins de vengeance, de sabotage ou d'espionnage

▶ Criminel

EX: Violence, fraude, vol de biens du MDN ou des FAC

Indicateurs comportementaux

Signalez tout changement et toute préoccupation de sécurité:

- Changements importants de situation personnelle ou de comportement (abus de drogues ou d'alcool/absences fréquentes inexplicables, richesse ou dettes inexplicables)
- Loyautés et obligations partagées envers des membres de la famille à l'étranger
- Problèmes relatifs à la sécurité (série de manquements à la sécurité, non-respect délibéré, non-respect des politiques)
- Recherche, demande, conservation ou accès non autorisés à des renseignements classifiés ou sensibles
- Incidents de sécurité inexplicables ou non signalée, ou proximité avec des menaces de sécurité connues.
- Expression continue d'un mécontentement à l'égard de son unité ou de son employeur
- Travail inexplicable ou inhabituel pendant les heures non surveillées
- Voyage à l'étranger ou contact avec des personnes étrangères non expliqué ou non déclaré (lorsqu'une déclaration est requise)
- Comportement suspect au travail (cacher des documents, masquer l'écran d'ordinateur, éviter les collègues)
- Activité ou profil en ligne atypique (utilisation du « dark web », contacts à l'étranger)
- Activité criminelle ou démêlés avec la justice (nouveaux/précédemment dissimulés)

N'oubliez pas de :

- ▶ Protéger les renseignements, ressources et systèmes du MDN/FAC
- ▶ Suivre la formation sur la sécurité
- ▶ Suivre les règles de SECOP (ne pas tenir les portes sécurisées, vérifier les éléments inconnus)
- ▶ Présenter un Avis d'intention de voyager (AIV) avant de voyager
- ▶ Toujours appliquer le principe du besoin de connaître lorsque vous faites part de renseignements sensibles ou que vous discutez de ceux-ci sur le lieu de travail

Signaler les préoccupations internes

Voies officielles:

1. Votre chaîne de commandement/superviseur
2. Surveillant de la sécurité de l'unité (SSU)
3. Officier de la sécurité des systèmes d'information (OSSI)
4. Soumettre un rapport sur un changement de situation (formulaire DND 4151)
5. Unité nationale de contre-ingérence des FC (UNCIFC) cfnciuops-opsuncifc@forces.gc.ca
6. Bureau des enquêtes administratives (BEA) du DGSD rod-rdd@forces.gc.ca
7. Groupe de la Police militaire des Forces canadiennes (Gp PM FC)

Superviseurs à tous les niveaux:

Aidez à réduire les risques internes!