



CENTRE
DE RÉADAPTATION
DE L'OUEST DE MONTRÉAL

WEST MONTREAL
READAPTATION
CENTRE

La sécurité des actifs informationnels, c'est l'affaire de tous !

Le personnel du CROM utilise quelque 300 ordinateurs personnels et portables, l'Internet et autres outils informatiques pour pouvoir exercer leurs fonctions.

Ces outils représentent une valeur légale, administrative et économique importante, voire inestimable.

Étant donné que notre centre doit protéger ses systèmes informatiques et que plusieurs lois, règlements et directives régissent la confidentialité de notre information, nous devons tous être extrêmement vigilants lorsque nous nous en servons.

Les politiques de sécurité au CROM :

- Changez souvent votre mot de passe et n'acceptez jamais de le prêter à qui que ce soit. Les meilleurs mots de passe comportent huit caractères et plus, des chiffres et des caractères spéciaux, ainsi que des lettres majuscules et minuscules. Évitez de l'écrire sur papier.
- N'envoyez jamais des données confidentielles à un courriel qui ne se termine pas en « ssss.gouv.qc.ca ». Ceci est interdit parce que les courriels ne sont pas cryptés et ne sont donc pas sécuritaires.
- Si vous laissez votre ordinateur déverrouillé en absence prolongée, vous risquez de permettre à quelqu'un d'accéder à votre information ou de se servir de votre ordinateur à votre place.
- Informez tout de suite votre supérieur immédiat de tout bris de confidentialité et de toute situation qui pourrait affecter les actifs informationnels.

Saviez-vous que ?

Il y a une raison pour laquelle vous ne pouvez pas télécharger de logiciels à partir de vos postes de travail. Ces logiciels pourraient contenir des virus, empêcher que d'autres logiciels fonctionnent correctement ou transmettre des données confidentielles sans que vous en soyez conscients.

Un virus informatique pourrait paralyser tout le réseau en quelques minutes.

Il importe de suivre les meilleures pratiques :

- N'ouvrez jamais une pièce jointe qui vous semble suspecte, même si elle provient de quelqu'un à qui vous faites confiance. Elle pourrait être infectée d'un virus ou être sous le contrôle d'un pirate informatique.
 - Téléchargez uniquement des fichiers de sites Web dont le propriétaire est connu et bien établi.
 - Créez régulièrement des copies de sauvegarde de vos renseignements et fichiers qu'il serait grave de perdre (documents, images, liens préférés, courriels importants).
 - Assurez-vous que l'accès à vos fichiers est restreint.