Centre intégré universitaire de santé et de services sociaux de la Mauricie-et-du-Centre-du-Québec

Québec

Note de service

DESTINATAIRES : Le personnel et les gestionnaires

EXPÉDITEUR : Daniel Brouillette, directeur
Direction des ressources informationnelles

DATE : Le 19 mars 2020

OBJET : Mesures de sécurité à adopter lors du télétravail

La Direction des ressources informationnelles (DRI) désire vous informer des **règles de sécurité** à suivre par le personnel lors du télétravail.

Les règles d'utilisation générales se déclinent comme suit :

- Se conformer à la Politique de sécurité de l'information;
- Adopter un comportement similaire à celui adopté lors de votre présence physique au-bureau;
- Éviter d'utiliser les outils de collaboration, Office365, à des fins d'échanges d'informations confidentielles.
- Éviter l'utilisation des jetons de téléaccès, lorsque non requis, une simple connexion Internet suffit généralement à répondre à la majorité des besoins corporatifs. Le jeton de téléaccès doit être réservé, en priorité, au personnel médical, clinique ou autres employés identifiés dans le cadre des services essentiels;
- S'assurer de la sécurité de son réseau sans fil, par la présence d'un mot de passe robuste associé à un mécanisme de chiffrement fort;
- Prendre les mesures sécuritaires requises pour éviter qu'une tierce personne utilise votre jeton, soit :
  - ne pas partager son NIP;
  - ne pas partager ses questions et réponses secrètes;
  - conserver son NIP dans un endroit très sûr.
- Signaler immédiatement au centre de services de votre établissement, tout acte, susceptible de constituer une violation réelle ou présumée des règles de sécurité ainsi que toute anomalie pouvant nuire à la protection des actifs informationnels du ministère.

Règles d'utilisation de l'équipement informatique <u>fourni par l'organisation</u> :

- Veiller à la sécurité physique de l'équipement corporatif, en le gardant à proximité lors de vos déplacements;
- Éviter la navigation Internet sur des sites non reliés à votre emploi;
- Éviter de brancher tout périphérique amovible, source généralement d'infection (ex. : téléphone intelligent, clé USB, etc.);
- Ne jamais laisser sa session ouverte, sans surveillance, ni partager son équipement avec une tierce personne.

Règles d'utilisation à domicile de <u>son propre équipement informatique</u>, lorsqu'autorisé par votre organisation :

- S'assurer de l'activation d'une solution antivirale, la tenir à jour et configurer adéquatement ses paramètres de détection;
- Tenir votre système d'exploitation (Windows 10 ou tout autre système d'exploitation récent) à jour ainsi que toutes les applications requises dans l'exercice de vos fonctions;
- Éviter de sauvegarder localement des documents confidentiels, le cas échéant, s'assurer de les retirer, sitôt leur utilité n'étant plus requise;
- S'assurer de la présence du verrouillage automatique de la session.