Mesures de sécurité à adopter lors du télétravail

Préambule

Le ministère de la Santé et des Services sociaux (MSSS) offre à son personnel et celui du réseau de la santé et des services sociaux le privilège d'opter pour le télétravail, comme modèle d'organisation du travail. Bien que ce modèle suscite de nombreux avantages, il est nécessaire, sur le plan de la sécurité de l'information et de la protection de l'infrastructure technologique ministérielle et réseau, d'encadrer son utilisation.

Le présent document énonce des règles de sécurité à suivre par le personnel du MSSS et de son réseau lors du télétravail. Elles se déclinent comme suit :

Règles d'utilisation générales :

- Se conformer à la politique de sécurité de l'information ainsi qu'au cadre de gestion de la sécurité de l'information du ministère ou de l'établissement;
- Adopter un comportement similaire à celui adopté lors de votre présence physique au bureau;
- Prendre connaissance des termes et conditions d'utilisation des outils de collaboration ainsi que les capsules de formation[1], offertes par le MSSS;
- Éviter d'utiliser les outils de collaboration, Office365, à des fins d'échanges d'informations confidentielles, concernant un usager, s'il existe des processus d'affaires prévus à cet effet. En cas d'absence de tels processus d'affaires et si la situation l'exige, le MSSS autorise l'utilisation des outils de collaboration à cette fin;
- 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[2] associé à un mécanisme de chiffrement fort[3];
- 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 fourni par l'organisation :

- 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 de son propre équipement informatique, 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, lors d'inactivité prolongée.

---

[1] https://msss365.sharepoint.com/sites/MSSS-Collaboration-SPO/SitePages/Formation.aspx
[2] Consulter le document « MSSS-PR01-PRATIQUE RECOMMANDÉE Création d'un mot de passe robuste ».
[3] Utiliser le protocole WPA2 et la méthode de chiffrement AES.