COVID-19

ANNEXE - Informations aux employés

Direction des ressources informationnelles

23 mars 2020

Mesures de sécurité à adopter lors de l'utilisation du téléaccès

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.

Éviter qu'une tierce personne utilise le jeton téléaccès qui vous a été octroyé, 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 service à l'utilisateur (via octopus ou en composant le 1 844 400-AIDE (2433)), tout acte susceptible de constituer une violation réelle ou présumée des règles de sécurité, ainsi que toute anomalie pouvant nuire à la protection des infrastructures technologiques du CISSS du Bas-Saint-Laurent.

→ **En cas de doute, n'hésitez pas à faire une requête.**

Éviter d'utiliser le courriel (et tout autre outil de collaboration) à des fins d'échanges d'informations confidentielles s'il existe déjà un processus d'affaires prévu à cet effet.

→ **En cas d'absence d'un tel processus d'affaires et si la situation l'exige, le CISSS du Bas-Saint-Laurent autorise l'utilisation du courriel pour l'envoi d'une telle information, mais exige qu'elle soit dans un document protégé par un mot de passe et jointe au courriel. Le mot de passe doit être transmis idéalement par téléphone, sinon, dans un courriel subséquent.**

Règles d'utilisation de l'équipement informatique de 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.

Québec

COVID-19

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.

En complément d'information, nous vous invitons à consulter le lien suivant qui explique les risques reliés au télétravail et les mesures à adopter pour se protéger :

https://www.cyber.gc.ca/fr/orientation/problemes-de-securite-lies-au-teletravail-itsap10016