EN CYBERSÉCURITÉ
J'AI MON RÔLE À JOUER

BONNES PRATIQUES EN SÉCURITÉ DE L'INFORMATION
DESTINÉES AU PERSONNEL DE L'ORGANISATION

SIGNALER RAPIDEMENT LES INCIDENTS AUPRÈS DE VOTRE CENTRE DE SOUTIEN TECHNIQUE

Tout membre du personnel a l'obligation de signaler :

- tout acte susceptible de représenter une violation réelle ou présumée des règles de sécurité tel que le vol, l'intrusion dans un réseau, les dommages délibérés,l'utilisation abusive ou la fraude
- la perte ou le vol d'un ordinateur portable, d'un support électronique amovible, d'un cellulaire ou d'une tablette
- tout support électronique amovible trouvé. À ce propos, il est interdit de le brancher et d'essayer d'en lire le contenu

SÉCURISER L'INFORMATION AU TRAVAIL

- **S'identifier en tout temps** sur les lieux de travail (exemple : carte d'accès).
- **Fermer sa session de travail** chaque fois qu'on s'éloigne de son poste.
- Utiliser en tout temps le **service d'impression sécurisé**.
- Imprimer ou télécopier des documents contenant de l'information sensible seulement lorsqu'il s'agit d'une **situation indispensable**.
- Déchiqueter ou jeter dans des **bacs de recyclage sécurisés** les documents papier contenant des renseignements sensibles.
- Utiliser un réseau **Wi-Fi sécurisé**.
- S'assurer que seuls les membres du personnel ont accès à l'information et à l'équipement de l'organisation.
- S'assurer de la sécurité de tout document imprimé à l'extérieur des lieux de travail (exemple : ne pas imprimer des documents lorsqu'on est connecté à un réseau public).

UTILISER DU MATÉRIEL FOURNI PAR L'ORGANISATION

- **Accéder au réseau** uniquement par l'entremise des équipements fournis ou autorisés par l'organisation.
- Utiliser uniquement les **logiciels autorisés et fournis** par l'organisation.
- **S'authentifier** uniquement sur des sites dont la communication est chiffrée.

  Note : l'adresse Web doit débuter par HTTPS.
- Informer son gestionnaire si certains accès ne sont plus requis pour exécuter ses tâches.
- Conserver la configuration des appareils mobiles fournis par l'organisation et s'assurer d'en faire les mises à jour rapidement.
- Être l'**unique utilisateur** d'un appareil mobile fourni.
- Associer uniquement son appareil mobile à un périphérique Bluetooth autorisé et sous le contrôle l'organisation.

Votre gouvernement

Québec

EN CYBERSÉCURITÉ

J'AI MON RÔLE À JOUER

PROTÉGER SES IDENTIFIANTS ET SES MOTS DE PASSE

- **Toujours utiliser un mot de passe robuste et unique** pour chaque compte, qu'il soit professionnel ou personnel. (exemple : 7gH!k9@2mL#x).
- **Ne pas enregistrer un mot de passe** sur son ordinateur, son portable, sa tablette, son cellulaire ou tout autre périphérique.
- **Ne jamais partager ses identifiants**, ses mots de passe et ses dispositifs d'authentification avec quiconque.
- **Changer immédiatement son mot de passe** si l'on soupçonne qu'il est connu d'une autre personne.

RÉPERTORIER LES FICHIERS INDIVIDUELS ET PARTAGÉS

- S'assurer que la copie des documents confidentiels est effectuée vers des répertoires possédant les restrictions appropriées afin que seules les personnes autorisées puissent y accéder.
- Éviter la copie de fichiers dans les répertoires susceptibles de nuire au bon fonctionnement ou à la sécurité des infrastructures de l'organisation, notamment les fichiers exécutables, les scripts, les jeux ou tout autre fichier d'origine douteuse.
- S'assurer que l'information qu'on souhaite partager ne cause aucun préjudice à l'organisation (exemple : divulgation de renseignements personnels).

GÉRER DES DOCUMENTS SENSIBLES ET DES BOÎTES COURRIEL

- Toujours utiliser les informations organisationnelles à l'aide des **applications permises** par l'organisation.
- **Chiffrer les courriels** sur Outlook lorsqu'on doit absolument partager de l'**information sensible**.
- **Limiter la transmission** d'information ou de documents sensibles aux personnes autorisées.
- S'assurer que les documents numériques contenant de l'information sensible soient déposés dans une structure documentaire possédant les **restrictions d'accès appropriées**.
- **Réserver à des fins professionnelles** l'utilisation des boîtes courriel de l'organisation.
- **Ne transférer aucun** courriel ou document professionnel vers sa boîte courriel personnelle.
- **Éviter l'utilisation** d'une adresse courriel personnelle ou des services de courriel externes au réseau de l'organisation (exemples : Yahoo, Gmail et Hotmail) à des fins professionnelles.
- **Ne pas communiquer** de renseignements facilitant ou permettant l'accès au réseau de l'organisation (exemples : identifiant et mots de passe).
- **Faire preuve de vigilance** par rapport aux attaques par pourriels, aux courriels d'hameçonnage, aux chaînes de courriels et à toute autre forme de sollicitation suspecte.
- **Signaler tout courriel suspect** dans Outlook. Pour ce faire, à la section Protection, cliquer sur l'onglet Accueil, puis sur Signaler le message.
- Éviter l'ouverture ou le transfert de courriels (incluant les pièces jointes) acheminés par un **expéditeur inconnu ou non sollicité**.