UQAC

Utiliser des bonnes pratiques en sécurité de l'information contribue à réduire les risques d'incident.
Voici un tableau de rappel de quelques-unes des bonnes pratiques à adopter.

Authentification	Communication
✓ Choisissez des mots de passe robustes (longs et complexes) ✓ Choisissez des mots de passe différents pour chaque authentification ✓ Changez les mots de passe fréquemment ✓ Ne divulguez jamais votre mot de passe ✓ Changez le mot de passe si vous croyez que quelqu'un d'autre le connait ✓ Activez l'authentification à double facteur lorsqu'elle est disponible	✓ Soyez à l'affût des messages d'hameçonnage et de harponnage ✓ Assurez-vous de l'identité des personnes qui vous interpellent par téléphone, messagerie texte ou courriel ✓ Reconnaissez les indices des pourriels (sentiment d'urgence, mauvaise orthographe, salutation générique, adresse de l'expéditeur, signature) ✓ N'ouvrez pas les fichiers ou les hyperliens des messages non sollicités ✓ Demandez la raison avant la collecte de vos renseignements personnels et libre à vous de consentir ou non
Prévention	**Environnement professionnel**
✓ Mettez à jour vos appareils mobiles, vos ordinateurs et vos applications ✓ Utilisez un antivirus ✓ Activez le pare-feu ✓ Utilisez un compte avec des droits restreints, élevez les privilèges au besoin ✓ Stockez vos données de façon sécuritaire et sachez comment récupérer les copies de sauvegarde ✓ Chiffrez vos stockages mobiles (clés, disques, portables, tablettes, téléphones) ✓ Sécurisez l'accès à vos appareils mobiles (tablettes, téléphones) avec des mots de passe ✓ Supprimez l'information stockée avant de vous débarrasser de vos équipements	✓ Ne modifiez pas la configuration de vos équipements de travail fournis par le Service des Technologies de l'information ✓ Ne téléchargez pas de logiciels sans licences ✓ Verrouillez votre poste de travail quand vous devez vous absenter ✓ Libérez votre espace de travail des documents confidentiels, rangez-les en sécurité ✓ Évitez d'exposer la vue de votre écran ✓ Disposez des renseignements confidentiels en les déchiquetant ou les démagnétisant ✓ Utilisez les renseignements personnels pour les raisons de la collecte seulement ✓ Assurez-vous que l'accès aux renseignements personnels est limité ✓ Déclarer les incidents de sécurité de l'information
Réseaux sociaux	**Navigation**
✓ Évitez de publier votre absence de la maison ✓ Demandez la permission avant de publier la photo d'une autre personne ✓ Ne publiez pas d'informations, photos ou vidéos personnelles ou sensibles ✓ Méfiez-vous, vos contacts pourraient partager du contenu malveillant à leur insu ✓ Méfiez-vous des offres alléchantes	✓ Évitez de vous connecter à des réseaux WI-FI publics ou non sécurisés ✓ N'utilisez pas la fonction « Se souvenir de moi » sur le web. Saisissez vos informations d'authentification à chaque fois ✓ Supprimer votre historique de navigation en fermant votre session ✓ Saisissez vos informations personnelles ou de paiement seulement sur des pages sécurisées (https)