Bonnes pratiques pour éviter les chances d'un incident de confidentialité[1]

Se conformer aux différentes obligations de la loi 25 n'est pas suffisant pour bien protéger votre syndicat, souvent, les bonnes pratiques seront votre meilleur atout.

Pour les personnes qui travaillent et militent dans le syndicat

- Toutes les personnes de votre équipe n'ont pas besoin d'avoir accès aux données de votre syndicat. La cartographie que vous avez remplie pourra vous aider à déterminer qui a accès à quels renseignements.
- Sensibilisez et formez toutes les personnes de votre équipe, quel que soit leur poste, en fonction des besoins de votre syndicat.
- Mettre en place une procédure de retrait de l'accès aux données lors de départs.

Contrôles physiques

- Assurer un contrôle physique des accès aux locaux où sont hébergés des données de recherche ou des équipements permettant d'y accéder.
- Placer dans des locaux, des cabinets ou des classeurs sécurisés toute donnée non utilisée en format papier contenant des informations sensibles.

Configuration des postes de travail ou de l'appareil informatique

- Protéger tous les postes de travail ou appareil informatique accédant aux données de recherche par un mot de passe fort ou à authentification multiple
- Garder à jour le système d'exploitation ainsi que les logiciels des postes de travail ou appareil informatique et activer les mises à jour automatiques.
- Installer un antivirus sur tous les postes de travail ou appareil informatique.
- Activer le coupe-feu personnel sur tous les postes de travail ou appareil informatique.
- Configurer l'écran de veille des postes de travail ou appareil informatique de manière que le poste soit verrouillé et protégé par un mot de passe après une période d'inactivité de 15 minutes

[1] Pour les différentes bonnes pratiques de cette section, nous avons repris certains éléments des sites suivants :

- https://cybersecurite.uqam.ca/guide-de-bonnes-pratiques-pour-la-securite-informatique-des-donnees-de-recherche/
- https://www.bdc.ca/fr/articles-outils/blogue/liste-controle-pratiques-exemplaires-cybersecurite-peut-vous-aider-prevenir-attaques-contre-votre-entreprise
- https://www.pensezcybersecurite.gc.ca/fr/ressources/guide-pensez-cybersecurite-pour-les-petites-et-moyennes-entreprises

Stockage et contrôle de l'accès des données

- Éviter de stocker les données uniquement sur un poste de travail, un appareil informatique, une clé USB ou un disque dur externe. S'assurer d'avoir plusieurs copies des données. Privilégier le stockage des données sur un espace commun sur le réseau ou dans le *cloud*.

Transfert de fichiers à l'externe

- Réaliser tout transfert de données sensibles vers l'externe en utilisant un canal de communication chiffré ou en chiffrant les données avant leur envoi.
- Éviter l'utilisation de services de stockage externe (ex. Dropbox) pour partager des données sensibles