

## Politique de gestion des données personnelles

Proposée au CA : 24 octobre 2023 Résolution: 2023.10.10 Adopté par le CA : 24 octobre 2023	<b>Politique no. 3</b>
Responsable de l'application :	Direction générale

### Table des matières

Procédure de conservation, de destruction et d'anonymisation des renseignements personnels\_ 2

Procédure de demande d'accès aux renseignements personnels et de traitement des plaintes \_ 4

Procédure de demande de désindexation et de suppression des renseignements personnels \_\_ 7

Procédure de gestion des incidents de sécurité et violations des renseignements personnels \_\_ 9

Procédure de gestion du roulement du personnel \_\_\_\_\_ 11

Document à faire signer en cas de roulement de personnel \_\_\_\_\_ 13

Liste de bonnes pratiques et outils en ligne pour la protection des renseignements personnels14

## **Procédure de conservation, de destruction et d'anonymisation des renseignements personnels**

### **1. Préambule**

Le Centre d'action bénévole de Boucherville (CABB) reconnaît l'importance de se conformer à la loi 25 sur la gestion des données personnelles.

### **2. Objectif général**

Le but de cette procédure est de garantir la protection de la vie privée des individus et de se conformer aux obligations légales en matière de protection des renseignements personnels.

### **3. Portée**

La portée de cette procédure devrait couvrir l'ensemble du cycle de vie des renseignements personnels, depuis leur collecte jusqu'à leur destruction. Elle concerne tous les employés, bénévoles et parties prenantes impliquées dans la collecte, le traitement, la conservation, la destruction et l'anonymisation des renseignements personnels, conformément aux exigences légales et aux bonnes pratiques en matière de protection de la vie privée.

### **4. Définitions**

- Renseignements personnels : toute information permettant d'identifier, directement ou indirectement, une personne physique.
- Conservation : stockage sécurisé des renseignements personnels pendant la durée requise.
- Destruction : suppression, élimination ou effacement définitif des renseignements personnels.
- Anonymisation : processus de modification des renseignements personnels de manière à ne plus permettre en tout temps et de façon irréversible l'identification, directe ou indirecte, des individus concernés.

### **5. Procédures**

#### **5.1 Durée de conservation**

5.1.1 Les renseignements personnels ont été catégorisés de la façon suivante :

- renseignements concernant les employés de l'entreprise,
- renseignements concernant les membres du conseil d'administration,
- renseignements concernant les bénévoles,
- renseignements concernant les usagers.

5.1.2 La durée de conservation pour chacune de ces catégories a été établie de la façon suivante :

- Employés de l'entreprise : 7 ans après la fin d'emploi.
- Membres du C.A. : 7 ans après la fin du mandat.
- Bénévoles : variable en fonction du type de renseignement personnel.
- Usagers : variable en fonction du type de renseignement personnel.

Pour plus de détails, se référer à l'inventaire complet des renseignements personnels détenus.

[Loi 25 Inventaire rp co..xlsx](#)

#### **5.2 Méthodes de stockage sécurisé**

5.2.1 Les renseignements personnels se trouvent dans la base de données CABSYS.

5.2.2 Le degré de sensibilité de ce lieu de stockage a été établi.

5.2.3 Ce lieu de stockage, qu'il soit papier ou numérique, est adéquatement sécurisé.

5.2.4 L'accès à ce lieu de stockage a été restreint aux seules personnes autorisées.

### **5.3 Destruction des renseignements personnels**

5.3.1 Pour les renseignements personnels sur papier, ils devront être totalement déchiquetés.

5.3.2 Pour les renseignements personnels numériques, ils devront être totalement supprimés des appareils (ordinateurs, téléphones, tablettes, disques durs externes), des serveurs et des outils informatiques.

5.3.3 Un calendrier de destruction en fonction de la durée de conservation établie pour chaque catégorie de renseignements personnels est mis sur pieds et tenu à jour. Il est impératif de documenter les dates de destruction prévues.

5.3.4 Le CABB s'assure que les renseignements personnels ne puissent pas être récupérés ou reconstitués.

### **5.4 Anonymisation des renseignements personnels**

5.4.1 L'anonymisation des renseignements personnels ne se ferait que si le CABB souhaitait les conserver et les utiliser à des fins sérieuses et légitimes. Actuellement, le CABB n'envisage pas conserver des renseignements personnels.

5.4.2 Dans l'éventualité peu probable que le CABB déciderait de conserver des renseignements personnels, une méthode d'anonymisation desdits renseignements devrait alors être définie et mise en place.

5.4.3 Le cas échéant, le CABB s'assurerait que l'information restante ne permette plus de façon irréversible l'identification directe ou indirecte des individus concernés et s'assurerait d'évaluer régulièrement le risque de réidentification des données anonymisées en effectuant des tests et des analyses pour garantir leur efficacité.

### **5.5 Formation et sensibilisation du personnel**

5.5.1 Le CABB doit s'assurer de fournir une formation régulière aux employés sur la procédure de conservation, de destruction et d'anonymisation des renseignements personnels, ainsi que sur les risques liés à la violation de la vie privée, incluant également la sensibilisation du personnel aux bonnes pratiques de sécurité des données et à l'importance du respect des procédures établies.

## **Procédure de demande d'accès aux renseignements personnels et de traitement des plaintes**

### **1. Préambule**

Puisqu'une personne peut demander à accéder aux renseignements personnels qu'une organisation détient sur elle, ou pourrait également formuler des plaintes, il est important d'avoir des balises prédéfinies pour répondre à ce type de demande.

### **2. Objectif**

Le but de cette procédure est de garantir que toutes les demandes d'accès sont traitées de manière confidentielle, rapide et précise, tout en respectant les droits des individus concernés.

### **3. Portée**

La portée de cette procédure concerne la personne responsable du traitement des demandes d'accès et du traitement des plaintes, nommément la Direction générale, ainsi que les individus souhaitant accéder à leurs propres renseignements personnels.

### **4. Procédure de demande d'accès**

#### ***4.1 Soumission de la demande***

4.1.1 L'individu qui souhaite accéder à ses renseignements personnels doit soumettre une demande écrite à la Direction générale, laquelle est responsable de la protection des renseignements personnels de l'organisation. La demande peut être envoyée par courriel à [vieprivee@cabboucherville.ca](mailto:vieprivee@cabboucherville.ca) ou par courrier postal.

4.1.2 La demande doit clairement indiquer qu'il s'agit d'une demande d'accès aux renseignements personnels, et fournir des informations suffisantes pour identifier l'individu et les renseignements recherchés.

4.1.3 Ces informations peuvent inclure le nom, l'adresse ainsi que toute autre information pertinente pour identifier de manière fiable l'individu qui effectue la demande.

#### ***4.2 Réception de la demande***

4.2.1 Une fois la demande reçue, un accusé de réception est envoyé à l'individu pour confirmer que sa demande a été prise en compte.

4.2.2 La demande devra être traitée dans les trente (30) jours suivant sa réception.

#### ***4.3 Vérification de l'identité***

4.3.1 Avant de traiter la demande, l'identité de l'individu doit être vérifiée de manière raisonnable. Cela peut être fait en demandant des informations supplémentaires ou en vérifiant l'identité de l'individu en personne.

4.3.2 Si l'identité ne peut pas être vérifiée de manière satisfaisante, le CABB se réserve le droit de refuser de divulguer les renseignements personnels demandés.

#### ***4.4 Réponse aux demandes incomplètes ou excessives***

4.4.1 Si une demande d'accès aux renseignements personnels est incomplète ou excessive, le responsable de la protection des renseignements personnels communique avec l'individu pour demander des informations supplémentaires ou clarifications.

4.4.2 Le CABB se réserve le droit de refuser une demande si elle est manifestement abusive, excessive ou non justifiée.

#### **4.5 Traitement de la demande**

4.5.1 Une fois l'identité vérifiée, le responsable de la protection des renseignements personnels procède à la collecte des renseignements demandés en veillant à respecter les restrictions légales éventuelles.

#### **4.6 Examen des renseignements**

4.6.1 Avant de communiquer les renseignements personnels à l'individu, le responsable examine attentivement les informations pour s'assurer qu'elles ne contiennent pas de renseignements tiers confidentiels ou susceptibles de porter atteinte à d'autres droits.

4.6.2 Si des renseignements de tiers sont présents, le responsable évalue s'ils peuvent être dissociés ou s'ils doivent être exclus de la divulgation.

#### **4.7 Communication des renseignements**

4.7.1 Une fois les vérifications terminées, les renseignements personnels sont communiqués à l'individu dans un délai raisonnable, conformément aux exigences légales en vigueur.

4.7.2 Les renseignements personnels peuvent être communiqués à l'individu par voie électronique, par courrier postal sécurisé ou en personne, selon les préférences de l'individu et les mesures de sécurité appropriées.

#### **4.8 Suivi et documentation**

4.8.1 Toutes les étapes du processus de traitement de la demande d'accès aux renseignements personnels doivent être consignées de manière précise et complète.

4.8.2 Registre de suivi des demandes d'accès.

Les détails de la demande, les actions entreprises, les décisions prises et les dates correspondantes doivent être enregistrés dans un registre de suivi des demandes d'accès.

- Date de réception de la demande ;
- Date de l'accusé de réception ;
- Date de la vérification de l'identité ;
- Méthode de vérification de l'identité ;
- Décision – demande d'accès acceptée ou refusée ;
- Date de la communication des renseignements (si applicable).

#### **4.9 Protection de la confidentialité**

4.9.1 Tout le personnel impliqué dans le traitement des demandes d'accès aux renseignements personnels doit respecter la confidentialité et la protection des données.

#### **4.10 Gestion des plaintes et des recours**

4.10.1 Si un individu est insatisfait de la réponse à sa demande d'accès aux renseignements personnels, il doit être informé des procédures de réclamation et des recours disponibles devant la Commission d'accès à l'information.

4.10.2 Les plaintes doivent être traitées conformément aux politiques et procédures internes en matière de gestion des plaintes.

## **5. Procédure de traitement des plaintes**

### **5.1 Réception des plaintes**

5.1.1 Les plaintes peuvent être déposées par écrit, par téléphone, par courrier électronique ou via tout autre canal de communication officiel. Elles doivent être enregistrées dans un registre centralisé, accessible uniquement au personnel désigné.

5.1.2 Les employés doivent informer immédiatement la personne responsable de la réception des plaintes, nommément la Direction générale.

### **5.2 Évaluation préliminaire**

5.2.1 Le responsable désigné examine chaque plainte pour évaluer sa pertinence et sa gravité.

5.2.2 Les plaintes frivoles, diffamatoires ou sans fondement évident peuvent être rejetées. Toutefois, une justification doit être fournie au plaignant.

### **5.3 Enquête et analyse**

5.3.1 Le responsable chargé de la plainte mène une enquête approfondie en collectant des preuves, en interrogeant les parties concernées et en recueillant tous les documents pertinents.

5.3.2 Le responsable doit être impartial et avoir l'autorité nécessaire pour résoudre la plainte.

5.3.3 Le responsable doit maintenir la confidentialité des informations liées à la plainte et veiller à ce que toutes les parties impliquées soient traitées équitablement.

### **5.4 Résolution de la plainte**

5.4.1 Le responsable de la plainte propose des solutions appropriées pour résoudre la plainte dans les meilleurs délais.

5.4.2 Les solutions peuvent inclure des mesures correctives, des compensations financières ou toute autre action nécessaire pour résoudre la plainte de manière satisfaisante.

### **5.5 Communication avec le plaignant**

5.5.1 Le responsable de la plainte communique régulièrement avec le plaignant pour le tenir informé de l'avancement de l'enquête et de la résolution de la plainte.

5.5.2 Toutes les communications doivent être professionnelles, empathiques et respectueuses.

### **5.6 Clôture de la plainte**

5.6.1 Une fois la plainte résolue, le responsable de la plainte doit fournir une réponse écrite au plaignant, résumant les mesures prises et les solutions proposées.

5.6.2 Toutes les informations et documents relatifs à la plainte doivent être conservés dans un dossier confidentiel.

## **Procédure de demande de désindexation et de suppression des renseignements personnels**

### **1. Préambule**

Cette procédure vise à répondre aux craintes et aux préoccupations de confidentialité et de protection des renseignements personnels de nos bénévoles et usagers.

### **2. Objectif**

Le but de cette procédure est de fournir un mécanisme structuré pour gérer les demandes de désindexation et de suppression des renseignements personnels émanant de nos bénévoles et usagers.

### **3. Portée**

Cette procédure s'applique à la Coordonnatrice, expérience bénévole ainsi qu'à son équipe de bénévoles chargée de la gestion des demandes de désindexation et de suppression des renseignements personnels. Elle couvre toutes les informations publiées sur nos plateformes en ligne, y compris notre site web, nos applications mobiles, nos bases de données ou tout autre support numérique utilisé par nos bénévoles et usagers.

### **4. Définitions**

- Suppression des renseignements personnels : action d'effacer complètement les données, les rendant indisponibles et irrécupérables.
- Désindexation des renseignements personnels : retrait des informations des moteurs de recherche, les rendant moins visibles, mais toujours accessibles directement.

La suppression élimine définitivement les données, tandis que la désindexation limite leur visibilité en ligne.

### **5. Procédure**

#### **5.1 Réception des demandes**

- 5.1.1 Les demandes de désindexation et de suppression des renseignements personnels doivent être reçues par l'équipe responsable désignée.
- 5.1.2 Les bénévoles et usagers peuvent soumettre leurs demandes par le biais de canaux spécifiques tels que le formulaire en ligne, l'adresse courriel [vieprivee@cabboucherville.ca](mailto:vieprivee@cabboucherville.ca) ou le numéro de téléphone.

#### **5.2 Vérification de l'identité**

- 5.2.1 Avant de traiter la demande, l'identité de l'individu doit être vérifiée de manière raisonnable, en demandant des informations supplémentaires ou en vérifiant l'identité de l'individu en personne.
- 5.2.3 Si l'identité ne peut pas être vérifiée de manière satisfaisante, le CABB se réserve le droit de refuser de donner suite à la demande.

#### **5.3 Évaluation des demandes**

- 5.3.1 L'équipe responsable doit examiner attentivement les demandes et les renseignements personnels concernés pour déterminer leur admissibilité à la désindexation ou à la suppression.
- 5.3.2 Les demandes doivent être traitées de manière confidentielle et dans le respect des délais prévus.

#### **5.4 Raisons d'un refus**

5.4.1 Voici les raisons pour lesquelles le CABB pourrait refuser de supprimer ou de désindexer des renseignements personnels :

- Pour continuer à fournir des biens et des services au bénévole ou usager;
- Pour des raisons d'exigence du droit du travail;
- Pour des raisons juridiques en cas de litige.

#### **5.5 Désindexation ou suppression des renseignements personnels**

5.5.1 L'équipe responsable doit prendre les mesures nécessaires pour désindexer ou supprimer les renseignements personnels conformément aux demandes admissibles.

#### **5.6 Communication du suivi**

5.6.1 L'équipe responsable est chargée de communiquer avec les demandeurs tout au long du processus, en fournissant des confirmations d'accusé de réception et des mises à jour régulières sur l'état d'avancement de leur demande.

5.6.2 Tout retard ou problème rencontré lors du traitement des demandes doit être communiqué aux demandeurs avec des explications claires.

#### **5.7 Suivi et documentation**

5.7.1 Toutes les demandes de désindexation et de suppression des renseignements personnels, ainsi que les actions entreprises pour y répondre, doivent être consignées dans un système de suivi dédié.

5.7.2 Les enregistrements doivent inclure les détails des demandes, les mesures prises, les dates et les résultats des actions effectuées.



## Procédure de gestion des incidents de sécurité et violations des renseignements personnels

### 1. Préambule

Un plan d'intervention est essentiel pour gérer des cyberincidents de manière efficace. Dans ces moments de crise, on ne sait pas toujours comment agir et prioriser les actions. Un plan d'intervention vient réduire le stress d'oublier des aspects importants.

### 2. Objectif

Le but de cette procédure est de s'assurer que le CABB est prêt à intervenir en cas de cyberincident de manière à pouvoir reprendre rapidement ses activités.

### 3. Portée

La portée de cette procédure inclut tous les réseaux et systèmes, ainsi que les parties prenantes (usagers, bénévoles, partenaires, employés, sous-traitants, fournisseurs) qui accèdent à ces systèmes.

### 4. Reconnaître un cyberincident

Le CABB doit être à l'affût de tout signe indiquant qu'un incident de sécurité s'est produit ou est en cours.

- Activité excessive ou inhabituelle de la connexion et du système, notamment à partir de tout identifiant d'utilisateur (compte d'utilisateur) inactif.
- Accès distant excessif ou inhabituel. Cela peut concerner le personnel ou des fournisseurs tiers.
- L'apparition de tout nouveau réseau sans fil (Wi-Fi) visible ou accessible.
- Une activité inhabituelle liée à la présence de logiciels malveillants, de fichiers suspects ou de fichiers et programmes exécutables nouveaux ou non approuvés.
- Ordinateurs ou appareils perdus, volés ou égarés qui contiennent des données de cartes de paiement, renseignements personnels ou d'autres données sensibles.

### 5. Coordonnées des personnes-ressources

Rôle	Fonction	Téléphone	Adresse de courriel
Responsable de l'application de la politique et du traitement des incidents	Direction générale	450-655-9081	direction@cabboucherville.ca

### 6. Atteinte à la protection des renseignements personnels – Intervention spécifique

Dans le cas où un incident de sécurité est confirmé, il faudra effectuer les étapes suivantes :

- Compléter le registre d'incidents de confidentialité pour documenter l'incident : [Loi 25 Registre incidents confidentialité.xlsx](#)
- Examiner l'atteinte à la protection des renseignements personnels pour déterminer si des **renseignements personnels** ont été perdus en raison d'un accès ou utilisation non autorisé, d'une divulgation non autorisée ou de toute atteinte à la protection de ces renseignements personnels et qu'il existe un risque de préjudice sérieux pour les personnes concernées. Dans un tel cas, le signaler à la Commission de l'accès à l'information du Québec ainsi qu'aux personnes dont les renseignements personnels sont visés par l'incident.

## **7. Rançongiciel – Intervention spécifique**

Dans le cas où un incident de sécurité de rançongiciel s'est produit, il faudra effectuer les étapes suivantes :

- Déconnecter immédiatement du réseau les appareils visés par un rançongiciel.
- Ne RIEN EFFACER sur des appareils (ordinateurs, serveurs, etc.).
- Examiner le rançongiciel et déterminer comment il a infecté l'appareil pour aider à comprendre comment l'éliminer.
- Communiquer avec les autorités locales pour signaler l'incident et coopérer à l'enquête.

Une fois le rançongiciel supprimé, une analyse complète du système doit être effectuée à l'aide d'un antivirus, d'un anti-maliciel et de tout autre logiciel de sécurité le plus récent disponible afin de confirmer qu'il a été supprimé de l'appareil.

Si le rançongiciel ne peut pas être supprimé de l'appareil, il doit être réinitialisé au moyen des supports ou des images d'installation d'origine.

Si les données sont critiques et doivent être restaurées, mais ne peuvent être récupérées à partir de sauvegardes non affectées, rechercher les outils de déchiffrement disponibles sur **nomoreransom.org**.

La politique est de ne pas payer la rançon, sous réserve des enjeux en cause. Le CABB devra faire appel aux services d'un chef de projet expert en cyberattaques qui saura protéger les systèmes pour éviter toute nouvelle infection en mettant en œuvre des correctifs ou des rustines - *Programme destiné à corriger les défauts d'un logiciel, d'une application* - pour empêcher toute nouvelle attaque.

## **8. Piratage de compte – Intervention spécifique**

Dans le cas où un piratage de compte s'est produit, il faudra effectuer les étapes suivantes :

- Aviser nos bénévoles, usagers, employés et organismes avec qui nous travaillons qu'ils pourraient recevoir des courriels frauduleux la part du CABB, et spécifier de ne pas répondre ou cliquer sur les liens de ces courriels.
- Vérifier si on a encore accès au compte en ligne. Sinon, communiquer avec le support de la plateforme pour tenter de récupérer l'accès.
- Changer le mot de passe utilisé pour se connecter à la plateforme.
- Si le mot de passe est réutilisé ailleurs, changer également tous ces mots de passe.
- Activer le double facteur d'authentification pour la plateforme.
- Supprimer les connexions et les appareils non légitimes de l'historique de connexion.

## **9. Perte ou vol d'un appareil – Intervention spécifique**

Dans le cas où une perte d'équipement s'est produite, il faudra effectuer les étapes suivantes :

- Le vol ou la perte d'un bien, tel qu'un ordinateur, un ordinateur portable ou un appareil mobile, doit être signalé immédiatement aux autorités policières locales. Cela inclut les pertes/vols en dehors des heures d'ouverture normale et pendant les week-ends.
- Si l'appareil perdu ou volé contenait des données sensibles et qu'il n'est pas crypté, effectuer une analyse de sensibilité, du type et du volume des données volées, y compris les numéros de cartes de paiement potentiellement concernés.
- Dans la mesure du possible, verrouiller/désactiver les appareils mobiles perdus ou volés (p. ex. : téléphones intelligents, tablettes, ordinateurs portatifs, etc.) et procéder à un effacement des données à distance.

## **Procédure de gestion du roulement du personnel**

### **1. Préambule**

Le départ d'un membre du personnel peut entraîner des dommages intentionnels, accidentels ou une perte de données.

### **2. Objectif**

Le but de cette politique est d'établir une liste de contrôle au sein de l'organisation pour encadrer le départ d'un membre de l'équipe.

### **3. Portée**

La portée de cette procédure inclut tous les individus qui quittent l'organisation et qui possédaient des accès physiques aux appareils et systèmes de l'organisation, ou aux comptes et différentes plateformes de l'organisation.

### **4. Procédure**

#### **4.1 Entrevue de départ ou mise à pied**

4.1.1 Éteindre les ordinateurs et appareils professionnels de l'employé.

4.1.2 Désactiver l'accès de l'employé à tous les systèmes. Suivre la liste des rôles et des accès : [Loi 25 Inventaire rp co..xlsx](#)

4.1.3 Supprimer les données professionnelles des appareils appartenant aux employés :  
- Observer l'utilisateur supprimer les comptes de messagerie de son téléphone.

4.1.4 S'assurer que l'employé retourne tout équipement appartenant à l'organisation : ordinateurs portables, tablettes, clés USB, etc.

4.1.5 Compiler une liste de tous les emplacements où l'employé a stocké des données professionnelles, y compris les plateformes de stockage infonuagiques.

#### **4.2 Téléphone**

4.2.1 S'assurer que le numéro de téléphone de l'employé n'est pas transféré à un numéro externe, tel qu'un téléphone portable personnel.

4.2.2 Changer le mot de passe de la messagerie vocale.

4.2.3 Modifier le message vocal sortant conformément à vos directives de communication.

4.2.4 Désigner une personne pour surveiller la messagerie vocale jusqu'à ce que ce numéro de téléphone puisse être supprimé ou réaffecté.

#### **4.3 Accès aux courriels**

4.3.1 Ne jamais supprimer le compte courriel d'un employé, mais créer une boîte courriel partagée et bloquer les accès tel que mentionné plus bas.

4.3.2 Modifier le mot de passe du compte dans le système de courriels de l'organisation. Passer en revue la section 4.4 Accès au réseau et au Cloud avant de réactiver le compte.

4.3.3 Si l'employé a utilisé un téléphone mobile personnel ou une tablette pour accéder à sa messagerie professionnelle, effacer ou supprimer le compte de messagerie.

4.3.4 Créer un message d'absence pour le compte de messagerie.

4.3.5 Supprimer l'employé des listes de diffusion de courriels internes.

4.3.6 Supprimer l'employé des listes de diffusion de courriels spécialisées. S'assurer que quelqu'un d'autre est membre pour ne pas manquer ces communications.

4.3.7 Contacter les organismes avec lesquels l'employé a travaillé pour les informer du départ et leur fournir un nouveau contact.

4.3.8 Désigner quelqu'un et lui donner les accès pour surveiller le courrier électronique de l'employé. La boîte de courriels restera disponible 30 jours, après quoi le compte sera supprimé.

#### ***4.4 Accès au réseau et/ou au Cloud***

4.4.1 Supprimer l'employé de tous les groupes de contrôle d'accès pour la connexion au domaine de l'organisation, VPN, bureau à distance, système d'organisation et autres systèmes.

4.4.2 Déplacer tous les fichiers de travail qui ont pu être stockés en dehors des dossiers de sauvegarde principaux de l'organisation vers un emplacement central.

4.4.3 Révoquer l'accès de l'employé au compte infonuagique d'organisation.

4.4.4 Supprimer les fichiers de travail de tout compte de stockage personnel.

4.4.5 Confirmer qu'aucun logiciel d'accès à distance n'est installé sur les appareils (LogMeIn ou TeamViewer), que l'employé pourrait utiliser pour accéder à l'ordinateur ou au réseau.

**Annexe #1**  
**Document à faire signer en cas de roulement de personnel**

Attestation – Remise des biens et des données

Je soussigné(e), \_\_\_\_\_ atteste avoir remis au Centre d'action bénévole de Boucherville (CABB), l'ensemble des biens et des données lui appartenant, cela inclut les données pouvant se trouver sur mes appareils personnels.

J'atteste également n'avoir fait aucune copie de ces données.

Signé le \_\_\_\_\_, à \_\_\_\_\_

\_\_\_\_\_  
*(signature de l'employé.e)*

## Annexe #2

### Liste de bonnes pratiques et outils en ligne pour la protection des renseignements personnels

**Utiliser des mots de passe forts** : un mot de passe fort comporte entre 16 et 20 caractères, composé d'une combinaison de lettres, de chiffres et de caractères spéciaux. Éviter d'utiliser des informations personnelles évidentes et utiliser des mots de passe différents pour chaque compte.

**Gestionnaires de mots de passe** : Il est possible d'utiliser un gestionnaire de mots de passe tel que Dashlane, Bitwarden, NordPass, Keepass ou 1Password pour générer, stocker et gérer les mots de passe.

**Activer l'authentification à deux facteurs** : Activer les méthodes d'authentification à deux facteurs (2FA) lorsque cela est possible pour ajouter une couche de sécurité supplémentaire en demandant une deuxième preuve d'identité lors de la connexion.

**Messages suspects** : Courriels, messages instantanés et appels téléphoniques non sollicités demandant des informations personnelles. Ne jamais cliquer sur des liens suspects et ne pas ouvrir les pièces jointes de sources inconnues.

**Mise à jour régulière des logiciels** : Valider avec la compagnie informatique que les systèmes d'exploitation, applications et antivirus sont à jour en installant les dernières mises à jour et correctifs de sécurité.

**Limiter les informations personnelles partagées en ligne** : Éviter de publier des informations personnelles sensibles sur les réseaux sociaux ou d'autres plateformes en ligne : adresse, numéro de téléphone, détails financiers.

**Réseaux Wi-Fi sécurisés** : Éviter de vous connecter à des réseaux Wi-Fi publics pour effectuer des transactions sensibles ou accéder à des informations confidentielles. Privilégier les réseaux Wi-Fi protégés par mot de passe ou utiliser un VPN en tout temps.

**Suppression des cookies** : Utiliser les outils de nettoyage du système d'exploitation pour supprimer les cookies de suivi et les données de navigation stockées sur les appareils.

**VPN (Virtual Private Network)** : Utilisez un VPN pour chiffrer votre connexion Internet et protéger votre vie privée en ligne. Des services populaires tels que NordLayer, ExpressVPN ou CyberGhost offrent des fonctionnalités de protection de la vie privée.

**Extensions de navigateur de confidentialité** : Installer des extensions de navigateur telles que Privacy Badger, uBlock Origin ou HTTPS Everywhere pour bloquer les traqueurs publicitaires, les publicités intrusives et forcer les connexions sécurisées.

**Chiffrement des communications** : Utiliser des services de messagerie et de communication chiffrés, tels que Signal, WhatsApp (avec le chiffrement de bout en bout activé) ou Telegram (avec le chat secret activé), pour protéger la confidentialité de vos conversations.

**Informations de paiement en ligne** : Lors d'achats en ligne, s'assurer de le faire sur des sites sécurisés et fiables. Vérifier la présence d'un cadenas dans la barre d'adresse et utiliser des méthodes de paiement sécurisées, telles que PayPal ou les cartes de crédit protégées.

**Chiffrement des fichiers** : Utiliser des outils de chiffrement pour protéger les fichiers sensibles. Des logiciels tels que VeraCrypt, AxCrypt ou BitLocker permettent de créer des conteneurs chiffrés ou de crypter des fichiers individuels.

**Navigation privée** : Utiliser le mode de navigation privée ou incognito du navigateur pour limiter la collecte de données et de cookies pendant les sessions de navigation. Cela empêche également l'enregistrement de l'historique de navigation.

**Vérification des paramètres de confidentialité** : Passer en revue et ajuster les paramètres de confidentialité des comptes en ligne, tels que les réseaux sociaux, les services de messagerie et les applications, pour limiter la quantité d'informations personnelles partagées et restreindre l'accès aux données.

**Suppression des données personnelles** : Supprimer régulièrement les données personnelles inutiles ou sensibles stockées sur les appareils, tels que les anciens courriels, les fichiers temporaires, les caches de navigateur et les historiques de recherche.

**Formation à la sensibilisation à la cybersécurité** : Familiariser les employés avec les meilleures pratiques de cybersécurité en suivant des cours en ligne, en lisant des ressources fiables et en restant informés des dernières menaces et techniques d'attaque.

***Il est important de noter que la protection des renseignements personnels est un processus continu et qu'il est essentiel de rester vigilant et de se tenir au courant des dernières pratiques et outils de sécurité en ligne.***