m'îles lieux ensemble

TABLE DE QUARTIER

POLITIQUE de **CONFIDENTIALITÉ** des **RENSEIGNEMENTS PERSONNELS** et **PROCÉDURES**

De M'îles Lieux Ensemble

Adoptée par le Conseil d'Administration le 11 mars 2024.

Tables des Matières

Politique de confidentialité des renseignements personnels

M'Îles Lieux Ensemble s'engage à respecter la confidentialité de tous types de renseignements que nous recueillons, que nous détenons, que l'on utilise ou que l'on communique à des tiers. À partir de nos plateformes numériques, par courriel ou encore par téléphone.

Toutes les informations collectées et recueillies sont conservées de manière sécuritaire dans nos bases de données. Ainsi, notre politique tient compte des nouvelles dispositions de la loi 25 sur la protection des renseignements personnels et les documents électroniques.

Ci-dessous vous trouverez un détail de nos pratiques quant aux données personnelles que nous recueillons lorsque vous naviguez sur nos différentes plateformes, lorsque vous devenez un membre de MLE ou vous vous abonnez à notre infolettre.

1. Collecte des données

En général, vous pouvez circuler sur notre site internet sans avoir besoin d'entrer des renseignements personnels https://www.mileslieuxensemble.org/.

En visitant notre site internet, nous collectons habituellement les informations suivantes à des fins de statistique. Prenez note que votre anonymat est conservé en tout temps lorsque vous fréquentez notre site internet.

- Onglets que vous consultez
- Dates et heures de votre présence sur notre site
- La provenance de votre connexion (exemple : Laval, Montréal, etc.)
- Informations que vous recherchez sur notre site

Nous recueillons également vos données personnelles lorsque vous décidez de vous abonner à notre infolettre. Cela nous permet de conserver vos informations dans notre base de données et de vous transmettre les informations en lien avec notre organisme à travers une infolettre saisonnière. Notez que vous pouvez vous désabonnez en tout temps si vous le souhaitez et vous informations seront automatiquement retirées de notre base de données. Informations conservées : Nom, prénom et adresse courriel.

Vous trouverez ci-dessous une énumération détaillée des informations que vous conservons en lien avec nos services et nos activités :

- Adhésion en tant que membre :

  - Citoyen(ne) ou personne-ressource : nom, prénom, adresse courriel, numéro de téléphone, quartier
  - Partenaire ou associé(e) : nom de l'organisme, adresse de l'organisme, nom, prénom, courriel et cellulaire du (de la) représentant(e)
- Lors d'une demande d'aide d'un(e) citoyen(ne) : plusieurs données sensibles sont recueillies selon la situation

2. Tiers pouvant avoir accès à vos renseignements personnels

Les membres de l'équipe de M'Îles Lieux Ensemble ont accès à vos renseignements et il peut arriver que les parties suivantes puissent avoir accès à des informations vous concernant :

- Partenaires de projets dans le cas d'une collaboration qui nécessite vos données personnelles afin de vous offrir des meilleurs services ou produits. Nous nous assurons que ces derniers détiennent une politique de confidentialité et s'engagent à utiliser vos données pour répondre seulement à notre collaboration et à conserver vos données en toute sécurité et confidentialité.
- En vertu des lois applicables, nous serons obligés de révéler vos informations personnelles à un(e) conseiller(-ère) juridique, organisme gouvernemental ou toute autre autorité qui en demande l'accès dans le cadre légal.

Ainsi, seules les personnes autorisées peuvent avoir accès à vos données en respectant la politique de confidentialité.
Tout autre tiers n'aura pas accès à vos données à moins que vous en donniez l'autorisation.

3. Utilisation des données et cookies

M'Îles Lieux Ensemble collecte chaque renseignement avec votre accord. En acceptant les cookies ou encore en acceptant de recevoir de l'information ou en adhérant d'être membre, cela nous permet de recueillir certains renseignements vous concernant. Nous utilisons vos renseignements à des fins de statistiques pour nos bilans annuels et pour l'amélioration de nos différents services et des plateformes numériques.

Les cookies et les technologies de suivi qui font partie de nos divers sites internet permettent de bonifier votre expérience sur nos plateformes et ainsi de collecter les informations pertinentes sur votre utilisation. En tout temps, vous pouvez avoir accès aux cookies via vos paramètres de navigateur et les

désactiver si vous le désirez. Prenez note que cela peut avoir une incidence sur certaines fonctionnalités de nos sites internet.

Sachez que nous nous ne conservons que les informations nécessaires et pertinentes à notre cause. Toutes autres données non pertinentes ne sont pas conservées dans notre base de données et dans nos archives.

Nous tenons à la confidentialité de tous les renseignements personnels en notre possession, d'où nos dispositions et nos mesures pour conserver toutes les informations de manière en sécuritaires.

4. Les mesures de sécurité

Toutes les informations personnelles recueillies sont conservées dans nos bases de données sécurisées. Seuls certains membres du personnel de l'équipe peuvent avoir accès à vos données en cas de besoin.

Des codes d'accès et d'autres mesures sont mis en place pour empêcher tout accès non autorisé et pour permettre aux renseignements de demeurer de manière sécuritaire dans nos bases de données sans être endommagés ou transformés.

5. Liens vers les sites externes

Vous trouverez certains liens sur nos différents sites web qui mènent vers des sources externes. Prenez note que nous ne sommes pas responsables des politiques de confidentialités adoptées par les liens externes. Nous vous recommandons de prendre connaissance de leurs politiques en matière de renseignements personnels avant de naviguer sur leurs plateformes numériques.

6. Vos droits

Vous avez le droit en tout temps de faire une demande afin de prendre connaissance, de rectifier ou encore de supprimer les informations que nous disposons à votre sujet. Pour ce faire, nous vous invitons à prendre contact avec la personne responsable (voir 4.5). Toute demande en lien avec la politique des renseignements personnels est traitée dans les 30 jours suivant la réception de celle-ci.

Notez que vous avez le droit de supprimer votre consentement à l'utilisation de vos données personnelles. Cependant, dans certaines circonstances, le fait de suspendre votre consentement pourrait entrainer une inaccessibilité à certains de nos services et de nos produits qui vous sont fournis.

Procédures

Les procédures présentées ici constituent un ensemble d'outils à la disposition de l'organisation afin de mettre en place des mécanismes en but de respecter la politique de confidentialité des renseignements personnels décrite ci-dessus.

1. Procédure de conservation, de destruction et d'anonymisation des renseignements personnels

1.1. Aperçu

Il est important de mettre en place une procédure de conservation, de destruction et d'anonymisation des renseignements personnels pour garantir la protection de la vie privée des individus, se conformer aux lois sur la protection des renseignements personnels, prévenir les incidents de confidentialité impliquant des renseignements personnels et les atteintes à la sécurité, maintenir la confiance des partenaires et des citoyen(ne)s afin de protéger la réputation de l'organisation.

1.2. Objectif

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.

1.3. 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 employé(e)s 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.

1.4.Définitions

Renseignements personnels : toute information permettant d'identifier, directement ou indirectement, une personne physique.

Conservation : stockage sécurisé des renseignements personnels pendant la durée requise. Les éléments peuvent également être conservés en format électronique. Les mêmes règles s'appliquent, peu importe le format papier ou électronique.

Destruction : suppression, élimination ou effacement définitifs 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.

1.5. Procédures

1.5.1. Durée de conservation

Les renseignements personnels ont été catégorisés de la façon suivante :

- Renseignements concernant les employé(e)s de l'organisation;
- Renseignements concernant les membres du conseil d'administration;
- Renseignements concernant les membres de l'organisation;
- Renseignements concernant les citoyen(ne)s.

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

- Employé(e)s de l'entreprise : 7 ans après la fin d'emploi.
- Membres du C.A. : 7 ans après la fin du mandat.
- Membres : variable en fonction du type de renseignement personnel.
- Citoyen(e)s : variable en fonction du type de renseignement personnel.

Pour plus de détails, se référer à l'inventaire complet des renseignements personnels détenus. Attention des délais de conservation spécifiques peuvent s'appliquer.

1.5.2. Méthodes de stockage sécurisé

Les renseignements personnels se trouvent sur l'infonuagique de MLE.

Le degré de sensibilité de chacun de ces lieux de stockage a été établi.

Ces lieux de stockage, qu'ils soient papier ou numérique, sont adéquatement sécurisés.

L'accès à ces lieux de stockage a été restreint aux seules personnes autorisées.

1.5.3. Destruction des renseignements personnels

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

Pour les renseignements personnels numériques, ils devront être totalement supprimés des appareils (ordinateurs, téléphone, tablette, disque dur externe), des serveurs et des outils infonuagiques.

Le calendrier de destruction en fonction de la durée de conservation (1.5.1.) établi pour chaque catégorie de renseignements personnels devra être fait. Il est impératif de documenter les dates de destruction prévues.

Il faudra s'assurer que la destruction est réalisée de manière à ce que les renseignements personnels ne puissent pas être récupérés ou reconstitués.

1.5.4. Anonymisation des renseignements personnels

L'anonymisation des renseignements personnels ne devrait se faire que si l'organisation souhaite les conserver et les utiliser à des fins sérieuses et légitimes.

La méthode d'anonymisation des renseignements personnels choisie est la suivante:

- Utilisation de la première lettre du prénom suivi du nom de famille.
- Dans un fichier contenant la date de naissance des personnes, remplacer cette information par la seule année de naissance.

Il faudra s'assurer que l'information restante ne permette plus de façon irréversible l'identification directe ou indirecte des individus concernés. Il faut également s'assurer d'évaluer régulièrement le risque de réidentification des données anonymisées en effectuant des tests et des analyses pour garantir leur efficacité.

1.5.5. Formation et sensibilisation du personnel

Il faudra s'assurer de fournir une formation 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.

Cela inclut également la sensibilisation du personnel aux bonnes pratiques de sécurité des données et à l'importance du respect des procédures établies.

2. Procédure de demande d'accès aux renseignements personnels et de traitement des plaintes

2.1. Aperçu

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.

2.2. 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.

2.3. Portée

La portée de cette procédure concerne les acteurs internes responsables du traitement des demandes d'accès et du traitement des plaintes, ainsi que les individus souhaitant accéder à leurs propres renseignements personnels.

2.4. Procédure de demande d'accès

2.4.1. Soumission de la demande

L'individu qui souhaite accéder à ses renseignements personnels doit soumettre une demande écrite au responsable de la protection des renseignements personnels de MLE. La demande peut être envoyée par courriel ou par courrier postal.

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.

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.

2.4.2. Réception de la demande

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

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

2.4.3. Vérification de l'identité

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.

Si l'identité ne peut pas être vérifiée de manière satisfaisante, l'organisation peut refuser de divulguer les renseignements personnels demandés.

2.4.4. Réponse aux demandes incomplètes ou excessives

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

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

2.4.5. Traitement de la demande

Une fois l'identité vérifiée, le (la) responsable de la protection des renseignements personnels pour traiter les demandes d'accès aux renseignements personnels procède à la collecte des renseignements demandés.

Le (la) responsable consulte les dossiers pertinents pour recueillir les renseignements personnels demandés, en veillant à respecter les restrictions légales éventuelles.

2.4.6. Examen des renseignements

Avant de communiquer les renseignements personnels à l'individu, le (la) 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.

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

2.4.7. Communication des renseignements

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

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.

2.4.8. Suivi et documentation

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

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).

2.4.9. Protection de la confidentialité

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

2.4.10. Gestion des plaintes et des recours

Si une personne est insatisfaite de la réponse à sa demande d'accès aux renseignements personnels, elle doit être informée des procédures de réclamation et des recours disponibles devant la Commission d'accès à l'information.

Les plaintes doivent être traitées conformément aux politiques et procédures internes en matière de gestion des plaintes (section suivante).

2.5. Procédure de traitement des plaintes

2.5.1. Réception des plaintes

Si une personne est insatisfaite de la réponse à sa demande d'accès aux renseignements personnels, elle doit être informée des procédures de réclamation et des recours disponibles devant la Commission d'accès à l'information.

Les plaintes doivent être traitées conformément aux politiques et procédures internes en matière de gestion des plaintes (section suivante).

2.5.2. Évaluation préliminaire

Le(la) responsable désigné(e) examine chaque plainte pour évaluer sa pertinence et sa gravité.

Les plaintes frivoles, diffamatoires ou sans fondement évidents peuvent être rejetées. Toutefois, une justification doit être fournie au (à la) plaignant(e).

2.5.3. Enquête et analyse

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

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

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

2.5.4. Résolution de la plainte

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

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

2.5.5. Communication avec le (la) plaignant(e)

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

Toutes les communications doivent être professionnelles, empathiques et respectueuses.

2.5.6. Clôture de la plainte

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

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

3. Procédure de demande de désindexation et de suppression des renseignements personnels

3.1. Aperçu

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

3.2. 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 membres.

3.3. Portée

Cette procédure s'applique à l'équipe interne 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 membres.

3.4. 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.

3.5. Procédure

3.5.1. Réception des demandes

Les demandes de désindexation et de suppression des renseignements personnels doivent être reçues par l'équipe responsable désignée.

Les client(e)s peuvent soumettre leurs demandes par le biais de canaux spécifiques tels que l'adresse courriel dédiée ou le numéro de téléphone.

3.5.2. Vérification de l'identité

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.

Si l'identité ne peut pas être vérifiée de manière satisfaisante, l'organisation peut refuser de donner suite à la demande.

3.5.3. Évaluation des demandes

Le (la) responsable doit examiner attentivement les demandes et les renseignements personnels concernés pour déterminer leur admissibilité à la désindexation ou à la suppression.

Les demandes doivent être traitées de manière confidentielle et dans le respect des délais prévus.

3.5.4. Raisons d'un refus

Il existe aussi des raisons parfaitement valables pour lesquelles nous pourrions refuser de supprimer ou de désindexer des renseignements personnels:

- Pour continuer à fournir des biens et des services au (à la) client(e) ;
- Pour des raisons d'exigence du droit du travail ;
- Pour des raisons juridiques en cas de litige.

3.5.5. Désindexation ou suppression des renseignements personnels

Le (la) responsable doit prendre les mesures nécessaires pour désindexer ou supprimer les renseignements personnels conformément aux demandes admissibles.

3.5.6. Communication du suivi

Le (la) responsable est chargé(e) de communiquer avec les demandeurs(-deuses) 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.

Tout retard ou problème rencontré lors du traitement des demandes doit être communiqué aux demandeurs(-deuses) avec des explications claires.

3.5.7. Suivi et documentation

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.

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

4. Procédure de gestion des incidents de sécurité et violations des renseignements personnels

4.1. Aperçu

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.

4.2. Objectif

Le but de cette procédure est de s'assurer que M'Îles Lieux Ensemble est prête à intervenir en cas de cyberincident de manière à pouvoir reprendre rapidement ses activités.

4.3. Portée

La portée de cette procédure inclut tous les réseaux et systèmes, ainsi que les parties prenantes (membres, partenaires, employé(e)s, fournisseurs) qui accèdent à ces systèmes.

4.4. Reconnaître un cyberincident

Un incident de cybersécurité peut ne pas être reconnu ou détecté immédiatement. Toutefois, certains indicateurs peuvent être les signes d'une atteinte à la sécurité, qu'un système a été compromis, d'une activité non autorisée, etc. Il faut toujours être à l'affût de tout signe indiquant qu'un incident de sécurité s'est produit ou est en cours.

Certains de ces indicateurs sont décrits ci-dessous :

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

4.5. Coordonnées des personnes-ressources

Rôle	Nom	Téléphone	Adresse courriel
Responsable du traitement des incidents	Linda Bernard	514-659-0333	direction@mileslieux ensemble.org
Direction	Linda Bernard	514-659-0333	direction@mileslieux ensemble.org
Responsable des communications	Emma Glémot	514-659-0333	developpement@miles lieuxensemble.org

4.6. Atteinte à la protection des renseignements personnels - intervention spécifique

S'il a été confirmé qu'un incident de sécurité lié à une atteinte à la protection des renseignements personnels s'est produit, il faudra effectuer les étapes suivantes :

- Compléter le registre d'incidents de confidentialité pour documenter l'incident.
- 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 autorisée, 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 au Québec.
  - Et, le signaler également aux personnes dont les renseignements personnels sont visés par l'incident.

4.7. Rançongiciel - intervention spécifique

S'il a été confirmé qu'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 vos appareils (ordinateurs, serveurs, etc.).
- Examiner le rançongiciel et déterminer comment il a infecté l'appareil. Cela vous aidera 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 (souvent le cas avec les programmes malveillants furtifs), l'appareil doit être réinitialisé au moyen des supports ou des images d'installation d'origine.
- Avant de procéder à la réinitialisation à partir de supports/images de sauvegarde, vérifier qu'ils ne sont pas infectés par des maliciels.
- 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. Il est également fortement recommandé de faire appel aux services d'un chef de projet expert en cyberattaques.
- Protéger les systèmes pour éviter toute nouvelle infection en mettant en œuvre des correctifs ou des rustines pour empêcher toute nouvelle attaque.

4.8. Piratage de compte - intervention spécifique

S'il a été confirmé qu'un piratage de compte s'est produit, il faudra effectuer les étapes suivantes :

- Aviser nos contacts et nos partenaires qu'ils pourraient recevoir des courriels frauduleux de notre part, 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.

4.9. Perte ou vol d'un appareil - intervention spécifique

S'il a été confirmé qu'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 portatif 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.

5. Procédure de gestion du roulement du personnel

5.1. Aperçu

Le départ d'un(e) membre du personnel peut entraîner des dommages intentionnels, accidentels ou une perte de données. Avec une liste de rôles et de leurs accès ainsi que d'une politique à appliquer avant un départ, vous pourrez éviter la plupart de ces pertes.

5.2. Objectif

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

5.3. 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.

5.4. Procédure

5.4.1. Entrevue de départ ou de mise à pied

Éteindre les ordinateurs et appareils professionnels de l'employé(e).

Désactiver l'accès de l'employé(e) à tous les systèmes. Suivre la liste des rôles et des accès.

Supprimer les données professionnelles des appareils appartenant aux employé(e)s :

- Observer l'utilisateur(-trice) supprimer les comptes de messagerie de son téléphone.
- Une personne de l'équipe informatique peut le faire par effacement à distance, ce qui peut potentiellement supprimer des données personnelles (à utiliser avec prudence).

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

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

5.4.2. Téléphone

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

Changer le mot de passe de la messagerie vocale.

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

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

5.4.3. Accès aux courriels

Idéalement, ne jamais supprimer le compte courriel d'un(e) employé(e). La bonne pratique serait de créer une boîte courriel partagée et de bloquer les accès tels que mentionnés plus bas.

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 Nuage avant de réactiver le compte.

Si l'employé(e) a utilisé un téléphone mobile personnel ou une tablette pour accéder à sa messagerie professionnelle, effacer ou supprimer le compte de messagerie si ce n'est déjà fait.

Créer un message d'absence pour le compte de messagerie conformément aux directives de communication de votre organisation.

Supprimer l'employé(e) des listes de diffusion de courriels internes.

Supprimer l'employé(e) des listes de diffusion de courriels spécialisées. S'assurer qu'une autre personne est membre pour ne pas manquer ces communications.

Contacter les fournisseurs avec lesquels l'employé(e) a travaillé pour les informer du départ et leur fournir un nouveau contact.

Désigner une personne et lui donner les accès pour surveiller le courrier électronique de l'employé(e). Déterminer combien de temps la boîte de courriels restera disponible – 30 jours – après quoi le compte sera supprimé. S'assurer de faire un suivi après la période établie.

5.4.4. Accès au réseau et/ou au nuage

Supprimer l'employé(e) 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.

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.

Révoquer l'accès de l'employé(e) au compte infonuagique d'organisation.

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

Passer en revue les règles d'accès au pare-feu pour confirmer que l'utilisateur(-trice) ne dispose d'aucun autre accès, tel qu'un VPN direct depuis son pare-feu personnel à la maison.

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

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

6.1. Mots de passe forts

Utilisez des mots de passe comportant entre 16 et 20 caractères, composé d'une combinaison de lettres, de chiffres et de caractères spéciaux dans vos mots de passe. Évitez d'utiliser des informations personnelles évidentes et utilisez des mots de passe différents pour chaque compte.

6.2. Gestionnaires de mots de passe forts

Utilisez un gestionnaire de mots de passe tel que Dashlane, Bitwarden, NordPass, Keepass ou 1Password pour générer, stocker et gérer vos mots de passe.

6.3. Authentification à deux facteurs

Utilisez des méthodes d'authentification à deux facteurs (2FA) lorsque cela est possible. Cela ajoute une couche de sécurité supplémentaire en demandant une deuxième preuve d'identité lors de la connexion.

6.4. Vigilance face aux messages suspects

Soyez vigilant avec les courriels, les messages instantanés et les appels téléphoniques non sollicités demandant des informations personnelles. Ne cliquez pas sur les liens suspects et n'ouvrez pas les pièces jointes de sources inconnues.

6.5. Mise à jour des logiciels

Maintenez vos systèmes d'exploitation, vos applications et vos antivirus à jour en installant les dernières mises à jour et correctifs de sécurité. Les mises à jour contiennent souvent des correctifs pour les vulnérabilités connues. Une gestion proactive des mises à jour OS et matérielles limitent de beaucoup les risques de sécurité.

6.6. Partage limité des informations personnelles

Évitez de publier des informations personnelles sensibles, telles que votre adresse, votre numéro de téléphone ou vos détails financiers, sur les réseaux sociaux ou d'autres plateformes en ligne.

6.7. Réseaux Wi-Fi sécurisés

Évitez de vous connecter à des réseaux Wi-Fi publics pour effectuer des transactions sensibles ou accéder à des informations confidentielles. Privilégiez les réseaux Wi-Fi protégés par mot de passe ou utilisez un VPN en (presque) tout temps.

6.8. Suppression des cookies

Utilisez les outils de nettoyage du système d'exploitation pour supprimer les cookies de suivi et les données de navigation stockées sur vos appareils.

6.9. 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.

6.10. Extensions de navigateurs de confidentialité

Installez des extensions de navigateur tel que Privacy Badger, uBlock Origin ou HTTPS Everywhere pour bloquer les traqueurs publicitaires, les publicités intrusives et forcer les connexions sécurisées.

Cette politique est inspirée de celle de Mesprocedures et des Clubs 4-H du Québec.

Attestation – Remise des biens et des données

Je soussigné(e), _____ atteste avoir remis à l'organisation _____, 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 _____

_____
(signature de l'employé)