PROCÉDURE INTERNE LOI 25

► **ADOPTÉE LE 25 SEPTEMBRE 2023**

LE CALACS du Saguenay
C.P. 8351, Succursale Racine
Chicoutimi, QC, G7H 5C2

Table des matières

1. PRÉAMBULE

Depuis le 21 septembre 2021, la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (Loi 25) modernise l'encadrement applicable à la protection des renseignements personnels dans diverses lois, dont la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels dans le secteur privé*. Ces modifications amènent le CALACS du Saguenay à se doter d'une procédure interne concernant le traitement et la conservation des données personnelles afin de se conformer aux modifications de la loi.

Les changements de la loi ont amené l'organisme à poser des actions pour répondre aux exigences en ce qui concerne, entre autres :

- Le traitement des incidents affectant la confidentialité des renseignements personnels ;
- L'exigence qu'une évaluation des facteurs relatifs à la vie privée soit réalisée en certaines circonstances, notamment à l'égard de tout projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels ;
- Le consentement requis préalablement à une collecte, une utilisation ou une communication de renseignements personnels ;
- L'obtention du consentement du titulaire de l'autorité parentale ou du tuteur pour une collecte, une utilisation ou une communication de renseignements personnels concernant un mineur de moins de 14 ans ;
- Le droit d'une personne d'accéder à certains renseignements personnels informatisés la concernant dans un format technologique structuré et couramment utilisé ou d'en exiger la communication à un tiers ;
- La conservation des renseignements personnels ;
- La formation d'un comité sur l'accès à l'information et la protection des renseignements personnels ;
- La fonction de responsable de la protection des renseignements personnels.

2. Rôle et responsabilités des responsables de la protection des renseignements personnels

Toute entreprise est responsable de la protection des renseignements personnels qu'elle détient. La personne ayant la plus haute autorité veille à assurer le respect et la mise en œuvre de la *Loi sur la protection des renseignements personnels dans le secteur privé* (Loi sur le privé). Considérant que la Loi 25 exige une désignation expresse pour le cas où la plus haute autorité d'une entreprise choisirait de déléguer cette fonction, la collective du CALACS du Saguenay doit s'assurer que la personne ainsi désignée aura les compétences et le temps nécessaires pour s'y consacrer. En effet, même si cette tâche est déléguée, la plus haute autorité de l'organisme, soit la présidente de la collective, demeure responsable de la protection des renseignements personnels. En date du 5 juillet 2023, conformément à l'article 3.1 de la *Loi sur la protection des renseignements personnels dans le secteur privé*, la collective du CALACS du Saguenay nomme Joannie Dionne, responsable des ressources humaines (intérim), et Christine Tremblay, coordonnatrice clinique, à titre de responsable de la protection des renseignements personnels (RPRP). Madame Tremblay veillera aux données liées aux services d'aide et madame Dionne s'occupera de celles liées aux ressources humaines, financières et aux autres volets de services.

En tant que RPRP, leur rôle est d'assurer la protection des renseignements personnels détenus par l'organisme et d'assurer la mise en œuvre de la loi ci-haut mentionnée.

Leurs principales responsabilités sont de :

- Mettre en place des règles de gouvernance en matière de protection des renseignements personnels au sein de l'organisme et de maintenir la conformité dans le temps ;
- Déterminer les responsabilités des membres du personnel en matière de protection des renseignements personnels ;
- Veiller à la formation et à la sensibilisation des employées et militantes quant à leur rôle et leurs responsabilités dans la protection des renseignements personnels et à l'application des règles de protection lors des traitements que peuvent subir les renseignements personnels tout au long de leur cycle de vie ;
- Intervenir pour faire des recommandations lors de l'instauration de nouveaux programmes automatisés impliquant des renseignements personnels ;
- Effectuer l'évaluation des facteurs relatifs à la vie privée lorsque surviennent des incidents impliquant la compromission de renseignements personnels et prendre la charge administrative de la déclaration des incidents ;
- Instaurer et chapeauter le processus de gestion des plaintes dirigées envers le CALACS du Saguenay (personnes fréquentant l'organisme, partenaires, etc.).

3. Procédure de conservation et de destruction des renseignements personnels (RP)

3.1. Objectif

Cette section de la politique permet d'établir les mesures pour la conservation et la destruction des renseignements personnels (RP) conformément aux exigences de la Loi 25. Elle couvre les informations importantes du cycle de vie des renseignements personnels, depuis leur collecte jusqu'à leur destruction. Elle concerne toutes les employées et parties prenantes impliquées dans la collecte, le traitement, la conservation et la destruction des renseignements personnels conformément aux exigences légales et aux bonnes pratiques en matière de protection de la vie privée.

3.2 Définitions

Renseignements personnels (RP) : 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.

3.3 Cycle de vie des données confidentielles

Source : [Protection des renseignements personnels | Commission d'accès à l'information du Québec (gouv.qc.ca)]

A) Collecte de données

Le CALACS du Saguenay recueille des données personnelles auprès des personnes qui fréquentent les services (ex. : nouvelle demande de service et création d'un dossier), des militantes (ex. : formulaire d'adhésion) et des employées (ex. : dossier employée). Le fait de visualiser un renseignement personnel sans la conservation de cette information demeure une collecte de données (ex : accompagnement formulaire IVAC). Le CALACS du Saguenay respecte ses obligations afin de protéger tous les renseignements personnels en ayant déterminé la pertinence des données recueillies au sein de l'organisme. Les renseignements personnels sont collectés uniquement à des fins légitimes et pertinentes. L'organisme possède une politique de confidentialité et un code d'éthique qui sont rigoureusement

appliqués par les employées et militantes. Chaque année, les employées et militantes doivent signer leur adhésion aux politiques internes de l'organisme.

Lors de collecte de données, les personnes sont informées de la finalité de leur utilisation et signent un formulaire de consentement[1].

Le CALACS du Saguenay s'est doté d'un guide d'utilisation des outils pour la tenue de dossier pour les travaux afin d'encadrer les pratiques pour respecter les normes et lois en vigueur. Les personnes fréquentant nos services sont informées à l'aide du guide d'accueil remis lors de la première rencontre d'intervention des informations suivantes :

- L'objet du dossier ;
- L'utilisation qui sera faite des renseignements personnels ;
- Les catégories de personnes qui y auront accès au sein de l'organisme ;
- L'endroit où ils seront détenus ;
- Ses droits d'accès et de rectification.

B) Durée de conservation

La durée de conservation des renseignements personnels a été catégorisée de la façon suivante :

- Renseignements concernant les employées de l'organisme ;
- Renseignements concernant les administratrices de la collective ;
- Renseignements concernant les membres de l'organisation (militantes) ;
- Renseignements concernant les personnes fréquentant nos services d'aide directe.

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

1) Employées du CALACS du Saguenay[2] : la coordonnatrice du CALACS du Saguenay et l'agente administrative sont les personnes ayant accès aux dossiers des employées. Elles veillent à leur conservation durant la période établie par la loi.
    - L'article 4 du *Règlement de formations admissibles* prévoit de conserver les informations quant aux formations qui ont été suivies pendant une durée de six (6) ans après la dernière année à laquelle des renseignements s'y rapportent.
    - La *Loi sur le ministère du Revenu* ainsi que la *Loi de l'impôt sur le revenu* prévoient de conserver le registre fiscal, ainsi que toutes les pièces à l'appui, pour une durée de six (6) ans après la dernière année à laquelle ils se rapportent ou six (6) ans après la production de la déclaration d'impôt.

[1] Pour les personnes fréquentant les services, le document interne se nomme « Attestation de réception d'information et consentement ». Pour les militantes, le document se nomme « contrat d'engagement – membre militante ». Pour les nouvelles employées, le document se nomme « Accueil et intégration RH ».

[2] Pourquoi conserver les dossiers de vos employés? (groupetcj.ca)

- La *Loi sur l'assurance-emploi* prévoit de conserver les relevés d'emploi et autres documents relatifs aux contributions, déductions ou réclamations pendant une période de six (6) ans après la fin de l'année à laquelle ils se rapportent jusqu'à ce qu'une décision soit rendue, y compris l'expiration du délai d'appel lors d'un litige en vertu des articles 90 et 91 de ladite loi.
- Le *Règlement sur la tenue d'un système d'enregistrement ou d'un registre*, à son article 2, prévoit une conservation obligatoire de trois (3) ans des registres de paie ainsi qu'à tous les documents y étant reliés. Cependant, un délai minimum de quatre (4) ans après la fin de l'exercice de l'année de terminaison d'emploi serait pertinent, et ce, selon l'article 66 de la *Loi sur le régime des rentes du Québec*.
- L'article 2925 du Code civil du Québec prévoit une prescription de trois (3) ans si nous mettons fin à l'emploi d'une employée. Il serait donc de mise de conserver les dossiers de nos employées congédiées pendant une période minimum de trois (3) ans à compter de la terminaison de l'emploi.
- La *Loi sur les assurances* ne prévoit aucune durée obligatoire quant à la conservation de l'information dans les dossiers des employées ayant une assurance collective. Le CALACS s'assure de respecter le contrat d'assurance collective pour la durée de conservation desdits dossiers.
- La *Loi sur les accidents du travail et les maladies professionnelles* prévoit de garder les dossiers médicaux des employées conservés pendant une durée de vingt (20) ans après la fin de l'emploi de l'employée ou une durée de quarante (40) ans après le début de son emploi, selon l'option la plus longue.

2) Administratrices : les membres de la collective, la coordonnatrice, l'agente administrative et la responsable de la lutte et de la vie associative sont les personnes ayant accès aux informations.

    - Le dossier est conservé pour une durée de sept (7) ans après la fin du mandat.

3) Membres militantes : la coordonnatrice, l'agente administrative et la responsable de la lutte et de la vie associative sont les personnes ayant accès aux informations.

    - La conservation est variable en fonction du type de renseignement personnel. Tout de même, nous gardons le dossier pour une durée de cinq (5) ans suivant l'année financière en cours.

4) Personnes fréquentant les services d'aide directe : la coordonnatrice clinique, les intervenantes sociales effectuant de l'aide directe et l'agente administrative au besoin ont accès aux dossiers et aux renseignements personnels.

    - La conservation des renseignements est variable en fonction du type de renseignement personnel. Selon les politiques internes mises en place, le dossier de chaque personne en suivi est conservé dans le classeur verrouillé de l'intervenante qui est attitrée à la situation

lorsque celui-ci est actif. Seules l'intervenante au dossier ainsi que l'agente administrative connaissent l'emplacement de la clé pour y avoir accès. Il importe que l'agente administrative soit mise au courant de l'emplacement de la clé advenant un empêchement ou une urgence faisant en sorte que l'intervenante soit dans l'impossibilité de se présenter à la rencontre prévue. L'agente pourra donc prévenir la personne en ayant accès aux coordonnées pour la rejoindre. À l'exception d'urgences de la sorte, l'agente ne consultera pas les dossiers.

- Suivant un délai de trois (3) mois d'inactivité, le dossier est considéré comme étant fermé et ce dernier est archivé dans un classeur commun verrouillé. Le dossier sera conservé au CALACS du Saguenay pendant une période de cinq (5) ans suivant le dernier contact, après quoi, il sera détruit de façon sécuritaire. Toutes les intervenantes du CALACS du Saguenay sont tenues de respecter la confidentialité au sujet des dossiers et de tout autre renseignement concernant les personnes qui fréquentent les services.

Pour plus de détails, se référer à l'inventaire complet des renseignements personnels détenus où l'on retrouve les détails concernant la conservation précise des RP. L'inventaire des renseignements personnels permet de connaître l'endroit où se trouvent ceux-ci. Le degré de sensibilité de chacun de ces lieux de stockage a été établi. De plus, qu'ils soient papier ou numérique, ces lieux de stockage sont adéquatement sécurisés et l'accès à ces lieux de stockage a été restreint aux seules personnes autorisées.

C) Destruction

Pour les renseignements personnels sur papier, ils devront être totalement déchiquetés. Pour les renseignements personnels numériques, ils devront être totalement supprimés des appareils (ordinateur, téléphone, tablette, disque dur externe), des serveurs et des outils infonuagiques. Les RPRP sont tenues de s'assurer que le calendrier de destruction est appliqué. Les méthodes utilisées sont réalisées de manière que les renseignements personnels ne puissent pas être récupérés ou reconstitués.

Le calendrier de destruction établit la durée de conservation pour chaque catégorie de renseignements personnels. Il documente les dates de destruction prévues. Pour plus de détails, se référer au document « Calendrier de destruction des RP ».

3.4 Formation et sensibilisation du personnel

Une formation est fournie par une responsable des renseignements lors de l'intégration d'une nouvelle employée et d'une nouvelle administratrice. De plus, une formation est fournie chaque année sur la procédure de conservation et de destruction 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. Les RPRP sont chargées de fournir ou mandater une organisation pour offrir cette formation.

4. Procédure de demande d’accès aux renseignements personnels et de traitement des plaintes

4.1 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.

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

4.2 Procédure de demande d’accès

4.2.1 Soumission de la demande

L'individu qui souhaite accéder à ses renseignements personnels doit soumettre une demande à une responsable de la protection des renseignements personnels (RPRP) de l’organisation. La demande peut être envoyée par courriel, par courrier postal ou remise en main propre. Pour ce faire, celle-ci doit en faire la demande par écrit en utilisant le formulaire de l’organisme (Annexe 1). Suivant la lecture de son dossier, la personne peut demander une rectification si elle juge que certaines informations sont manquantes, incorrectes ou non justifiées. Il est recommandé que la personne nomme ses rectifications par écrit.

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.

4.2.2 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. 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.

Si une demande d'accès aux renseignements personnels est incomplète ou excessive, la RPRP en charge du dossier communique avec l'individu pour demander des informations supplémentaires ou des clarifications. L'organisation se réserve le droit de refuser une demande si elle est manifestement abusive, excessive ou injustifiée.

4.2.3 Traitement de la demande

Une fois l'identité vérifiée, une RPRP procède à la collecte des renseignements demandés. La demande devra être traitée dans les trente (30) jours ouvrables suivant sa réception. La responsable consulte les dossiers pertinents pour recueillir les renseignements personnels demandés, en veillant à respecter les restrictions légales éventuelles. Avant de communiquer les renseignements personnels à l'individu, 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, la responsable évalue s'ils peuvent être dissociés ou s'ils doivent être exclus de la divulgation.

4.2.4 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.

Si la demande est acceptée, la personne pourra consulter son dossier sur les heures d'ouverture du CALACS du Saguenay. Si la personne demande à obtenir une copie, la responsable devra lui en procurer une sans frais. Seule une personne mineure de moins de 14 ans n'a pas accès à son dossier sans l'autorisation parentale.

4.2.5 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. Ainsi, les détails suivants doivent se retrouver dans le registre pour chaque demande :

- 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).

4.2.6 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. Se référer à la politique de confidentialité et au code d'éthique de l'organisme.

4.2.7 Gestion des plaintes et des recours

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

5. Procédure de traitement des plaintes

5.1 Objectif

Cette section permet de clarifier la marche à suivre pour le traitement d'une plainte.

5.2 Procédure

5.2.1 Réception des plaintes

Toute personne ayant des insatisfactions est invitée à s'adresser à la personne concernée par la situation. Si cette première démarche ne satisfait pas la personne, elle peut communiquer avec la présidente de la collective pour lui faire part de la situation. Si cette démarche ne permet pas de régler la situation, la personne peut aussi faire une plainte formelle au sein de l'organisme. Les plaintes seront enregistrées dans un registre centralisé, accessible uniquement au personnel désigné. L'utilisation d'un formulaire de dépôt de plainte est recommandée. Un exemplaire sera envoyé par courriel ou par la poste, ou il pourra être remis directement à la personne.

Les employées doivent informer immédiatement une des RPRP afin qu'elle assure la procédure de traitement des plaintes. La plainte sera transférée à la présidente de la collective. Un avis de réception sera envoyé par la présidente de la collective à la plaignante. Le délai de traitement d'une plainte est de trente (30) jours ouvrables à compter du jour de la transmission de l'avis de réception de la plainte.

5.2.2 Évaluation préliminaire

La présidente de la collective examine chaque plainte pour évaluer sa pertinence et sa gravité. Les plaintes diffamatoires ou sans fondement évident peuvent être rejetées. Toutefois, une justification doit être fournie à la personne plaignante.

5.2.3 Enquête et analyse

La présidente, en collaboration avec une RPRP au besoin, mène une enquête approfondie en collectant des preuves, en interrogeant les parties concernées et en recueillant tous les documents pertinents. La présidente se doit d'être impartiale et a l'autorité nécessaire pour résoudre la plainte.

La présidente et la RPRP vont maintenir la confidentialité des informations liées à la plainte et veiller à ce que toutes les parties impliquées soient traitées équitablement.

La présidente communiquera régulièrement avec la personne plaignante pour la tenir informée de l'avancement de l'enquête et de la résolution de la plainte.

5.2.4 Résolution de la plainte

La présidente de la collective propose des solutions appropriées pour résoudre la plainte dans les meilleurs délais. Une fois la plainte résolue, la présidente fournira une réponse écrite à la personne plaignante résumant les mesures prises et les solutions proposées. Toutes les informations et documents relatifs à la plainte doivent être conservés dans un dossier confidentiel par la RPRP au dossier.

Si la personne plaignante n'est pas satisfaite du résultat des démarches auprès de notre organisme, la RPRP lui fournira les informations sur le Commissaire régional aux plaintes et à la qualité des services.

6. Procédure de demande de suppression des renseignements personnels

6.1 Objectif

Cette procédure vise à répondre aux craintes et aux préoccupations de confidentialité et de protection des renseignements personnels des personnes fréquentant nos services ou s'impliquant dans notre organisme. Le but de cette procédure est de fournir un mécanisme structuré pour gérer les demandes 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 et papier utilisé par les personnes fréquentant ou s'impliquant dans notre organisme.

6.2 Définition

Suppression des renseignements personnels : action d'effacer complètement les données, les rendant indisponibles et irrécupérables.

6.3. Procédure

6.3.1 Réception des demandes

Les demandes de suppression des renseignements personnels doivent être reçues par l'une des RPRP de l'organisme. Les personnes peuvent soumettre leur demande par le biais du formulaire de l'organisme, par l'adresse courriel dédiée ou par appel téléphonique.

6.3.2 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.

6.3.3 Évaluation des demandes

La RPRP doit examiner attentivement les demandes et les renseignements personnels concernés pour déterminer leur admissibilité à la suppression. Les demandes doivent être traitées de manière confidentielle et dans le respect des délais prévus.

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 client ;
- Pour des raisons d'exigence du droit du travail ;
- Pour des raisons juridiques en cas de litige.

6.3.4 Suppression des renseignements personnels

La RPRP doit prendre les mesures nécessaires pour supprimer les renseignements personnels conformément aux demandes admissibles.

6.3.5 Communication du suivi

La RPRP est chargée de communiquer avec la personne demandeuse tout au long du processus en fournissant des accusés de réception et des mises à jour régulières sur l'état d'avancement de sa demande. Tout retard ou problème rencontré lors du traitement des demandes doit être communiqué à la personne demandeuse avec des explications claires.

6.3.6 Suivi et documentation

Toutes les demandes 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.

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

7.1 Objectif

Le but de cette procédure est de s'assurer que l'organisation est prête à intervenir en cas de cyberincident de manière à pouvoir reprendre rapidement ses activités. La portée de cette procédure inclut tous les réseaux et systèmes, ainsi que les parties prenantes (clients, partenaires, employées, sous-traitants, fournisseurs) qui accèdent à ces systèmes. Un registre d'incidents a été mis à place dans l'organisation et les lois seront appliquées si un incident lié à des renseignements personnels a lieu.

7.2 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 :

- 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 dans votre organisation. Cela peut concerner le personnel ou des fournisseurs tiers ;
- 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.

7.3 Coordonnées des personnes-ressources

Rôle	Nom	Téléphone	Adresse de courriel
Responsable du traitement des incidents	Joannie Dionne, RH intérim	418 545-6444 poste 207	joannie@calacsdusaguenay.ca
Responsable des TI	Blackburn et Blackburn	418 549-4900	pblackburn@blackburninc.com
Assureur en cybersécurité	Taillon assurance	418 275-2372 poste 322	claudia.turcotte@taillon.ca

7.4 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 :

1. Compléter le registre d'incidents de confidentialité pour documenter l'incident ;
2. Examiner l'atteinte à la protection des renseignements personnels pour déterminer si des renseignements personnels ont été perdus en raison d'un accès ou d'une 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 :
    a. Le signaler à la Commission de l'accès à l'information au Québec ;
    b. Le signaler également aux personnes dont les renseignements personnels sont visés par l'incident.

7.5 Rançongiciel – Intervention spécifique

S'il a été confirmé qu'un incident de sécurité de rançongiciel s'est produit, il faudra effectuer les étapes suivantes :

1. Déconnecter immédiatement du réseau les appareils visés par un rançongiciel ;
2. Ne RIEN EFFACER sur de vos appareils (ordinateurs, serveurs, etc.) ;
3. Examiner le rançongiciel et déterminer comment il a infecté l'appareil. Cela vous aidera à comprendre comment l'éliminer ;
4. Communiquer avec les autorités locales pour signaler l'incident et coopérer à l'enquête ;
5. Une fois le rançongiciel supprimé, une analyse complète du système doit être effectuée à l'aide d'un antivirus, d'un antimaliciel et de tout autre logiciel de sécurité le plus récent disponible afin de confirmer qu'il a été supprimé de l'appareil ;
6. Si le rançongiciel ne peut pas être supprimé de l'appareil, 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 ou des images de sauvegarde, vérifier qu'ils ne sont pas infectés par des maliciels ;

7. 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 ;
8. 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 (*breach coach*) ;
9. Protéger les systèmes pour éviter toute nouvelle infection en mettant en œuvre des correctifs ou des rustines pour empêcher toute nouvelle attaque.

*Il est à noter que l'assureur actuel de l'organisme ne couvre pas le rançongiciel.

7.6 Piratage de compte – Intervention spécifique

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

1. Aviser les personnes fréquentant ou s'impliquant dans l'organisme et les fournisseurs qu'ils pourraient recevoir des courriels frauduleux de notre part et spécifier de ne pas répondre ou cliquer sur les liens de ces courriels ;
2. Vérifier si on a encore accès au compte en ligne. Sinon, communiquer avec le support de la plateforme pour tenter de récupérer l'accès ;
3. Changer le mot de passe utilisé pour se connecter à la plateforme ;
4. Si le mot de passe est utilisé ailleurs, changer également le mot de passe des autres plateformes ;
5. Activer le double facteur d'authentification pour la plateforme ;
6. Supprimer les connexions et les appareils non légitimes de l'historique de connexion.

7.7 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 et vols en dehors des heures d'ouverture normales 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 ou perdues ;
- Dans la mesure du possible, verrouiller et désactiver les appareils mobiles perdus ou volés (ex. : téléphones intelligents, tablettes, ordinateurs, portatifs, etc.) et procéder à un effacement des données à distance.

8. Procédure de gestion du roulement du personnel

8.1 Objectif

Le départ d'une membre du personnel peut entraîner des dommages intentionnels, accidentels ou une perte de données. Le but de cette politique est d'établir une liste de contrôle au sein de l'organisation pour encadrer le départ d'une membre de l'équipe. 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.

8.2 Procédure

8.2.1 Entrevue de départ ou mise à pied

Éteindre les ordinateurs et appareils professionnels de l'employée.

Désactiver l'accès de l'employée à tous les systèmes. Suivre la liste des rôles et des accès.

Supprimer les données professionnelles des appareils appartenant aux employées :

- Observer l'utilisateur 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'employée retourne tout équipement appartenant à l'organisation : ordinateurs portables, tablettes, clés USB, etc.

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

8.2.2 Accès aux courriels

Modifier le mot de passe du compte dans le système de courriel de l'organisation.

Si l'employée a utilisé un téléphone mobile personnel ou une tablette pour accéder à sa messagerie professionnelle, effacer ou supprimer le compte de messagerie de l'appareil 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'employée des listes de diffusion des courriels internes.

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

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

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

8.2.3 Accès au réseau et/ou au compte infonuagique

Supprimer l'employée 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'employée au compte infonuagique de l'organisation.

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

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

9. Liste de bonnes pratiques et outils en ligne pour la protection des renseignements personnels mis en place au CALACS du Saguenay

- **Méfiez-vous des 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.

- **Mettez à jour régulièrement vos 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 limite de beaucoup les risques de sécurité.

- **Limitez les informations personnelles partagées en ligne** : 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.

- **Utilisez des 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.

- **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.

- **Soyez prudent avec les informations de paiement en ligne** : lorsque vous effectuez des achats en ligne, assurez-vous de le faire sur des sites sécurisés et fiables. Vérifiez la présence d'un cadenas

dans la barre d'adresse et utilisez des méthodes de paiement sécurisées, telles que PayPal ou les cartes de crédit protégées.

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

- **Vérification des paramètres de confidentialité** : Passez en revue et ajustez les paramètres de confidentialité de vos 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 à vos données.

- **Suppression des données personnelles** : Supprimez régulièrement les données personnelles inutiles ou sensibles stockées sur vos 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** : Familiarisez-vous avec les meilleures pratiques de cybersécurité en suivant des cours en ligne, en lisant des ressources fiables et en restant informé 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.