Politique de gouvernance

POLITIQUE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS (LOI 25)

Sous la responsabilité du Conseil d'administration

Numéro : 25-2024

adoptée le :

évaluée le :

1.0 Préambule

Conformément à la Loi 25, Culture Lanaudière s'engage à protéger la confidentialité et la sécurité des informations personnelles des personnes utilisant nos services. La présente politique vise à les informer sur la manière dont nous collectons, utilisons et partageons les informations, ainsi que sur les choix qui s'offrent à eux en ce qui concerne leurs données personnelles.

2.0 Collecte d'informations

Nous collectons des informations personnelles lorsque les personnes interagissent avec nous, que ce soit en ligne, par téléphone, en personne ou par d'autres moyens. Les informations que nous pouvons collecter comprennent, sans s'y limiter :

- Le nom, l'adresse, l'adresse électronique et le numéro de téléphone;
- Des informations sur leurs préférences et leurs intérêts culturels;
- Des informations sur leurs transactions avec nous.

2.1 Utilisation des informations

Nous utilisons les informations personnelles aux fins suivantes :

- Pour répondre aux demandes de renseignements et de services;
- Pour envoyer des informations sur nos activités, nos événements et nos programmes;
- Pour traiter les demandes, les services et les achats;
- Pour améliorer nos services et personnaliser l'expérience client;
- Pour respecter nos obligations légales.

2.2 Partage des informations

Nous ne partageons les informations personnelles qu'avec des tiers dans les cas suivants où la personne y consent expressément, soit :

- Lorsque cela est nécessaire pour fournir les services qu'on nous a demandés;
- Pour respecter nos obligations légales.

2.3 Sécurité des informations

Nous mettons en place des mesures de sécurité appropriées pour protéger les informations personnelles contre tout accès non autorisé, toute divulgation, toute altération ou toute destruction.

2.4 Conservation des informations

Nous conservons les informations personnelles aussi longtemps que nécessaire pour atteindre les finalités pour lesquelles elles ont été collectées, sauf si une période de conservation plus longue est requise ou autorisée par la loi.

2.5 Durée de conservation

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 membres de l'organisation,
- Renseignements concernant les clients.

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 conseil d'administration : 7 ans après la fin du mandat.;
- Membres : variable en fonction du type de renseignement personnel.
- Clients : variable en fonction du type de renseignement personnel.

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

2.6 Méthodes de stockage sécurisé

- Les renseignements personnels se trouvent aux endroits suivants :
  - Dans les fiches personnelles complétées par la personne elle-même;
  - Dans les banques de métadonnées, créées suite aux fiches personnelle;
  - Dans les listes de contacts des employés;
- 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.

2.7 Destruction des renseignements personnels

- Pour les renseignements personnels sur papier, ils devront être totalement déchiquetés après la période définie de sept années;
- Pour les renseignements personnels numériques, ils devront être totalement supprimés des appareils (ordinateurs, téléphone, tablette, disque dur externe), des serveurs et des outils infonuagiques après la période définie de sept années;
- Le calendrier de destruction en fonction de la durée de conservation établie 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.

2.8 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 :
    - Catégoriser les informations par groupe d'âge, ou par territoire de MRC, en autant qu'il n'y a pas de possibilité d'identification à cause d'un nombre trop petit;
- Il faudra s'assurer que l'information restante ne permettre plus de façon irréversible l'identification directe ou indirecte des individus concernés et s'assurer d'évaluer régulièrement le risque de ré identification des données anonymisées en effectuant des tests et des analyses pour garantir leur efficacité.

2.9 Les droits et choix des utilisateurs

Les personnes qui utilisent nos services ont certains droits sur leurs informations personnelles, notamment :

- Le droit d'accéder à leurs informations personnelles;
- Le droit de rectifier leurs informations personnelles;
- Le droit de supprimer leurs informations personnelles;
- Le droit de s'opposer au traitement de leurs informations personnelles;
- Le droit de retirer leur consentement lorsque le traitement est fondé sur le consentement.

2.10 Formation et sensibilisation du personnel

- Il faudra 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;

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

- Idéalement, cette formation serait annuelle.

3. Responsable de la protection des renseignements personnels (RPRP)

En août 2022, conformément à la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (loi 25), une personne responsable de la

protection des renseignements personnels a été désignée au sein de notre organisation/entreprise.

Son rôle

La personne responsable de la protection des renseignements personnels s'assure que Culture Lanaudière réponde aux exigences légales en matière de renseignements, de protection, de collecte, d'utilisation, de communication et de destruction des renseignements personnels.

Chez Culture Lanaudière, par résolution du conseil d'administration, ce rôle est tenu par la direction générale en fonction : madame Andrée Saint-Georges

Sa mission

Au sein de notre organisation/entreprise, le/la RPRP :

- Tient à jour l'inventaire des renseignements personnels de Culture Lanaudière;
- Réalise et effectue les mises à jour de l'inventaire des plateformes utilisées par Culture Lanaudière;
- S'occupe de recevoir les questions, demandes, plaintes et commentaires de ses membres, partenaires et clientèles concernant leurs renseignements personnels, puis d'y répondre;
- Tient un registre d'incidents de confidentialité;
- Poursuit l'implantation de mesures de cyber sécurité et lui transmet les problèmes portés à sa connaissance;
- Contribue à la compréhension et au respect du protocole de gestion des incidents de sécurité par l'ensemble du personnel;
- Alerte et applique le protocole d'incident en cas de perte de renseignements personnels.
- Voit à l'application des procédures dans les cas de figure, tels que décrits dans le règlement affilié à cette politique.

Culture Lanaudière

Procédure de traitement des plaintes et de demande d'accès au renseignements personnels

Mars 2024 - Rédaction : l'équipe de Culture Lanaudière

1. Aperçu
Dans la mesure où une personne peut demander à accéder aux renseignements personnels que Culture Lanaudière détient sur elle, ou encore pourrait formuler une plainte, il est important d'avoir des balises prédéfinies pour y répondre.

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 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.

PROCÉDURE DE DEMANDE D'ACCÈS AU RENSEIGNEMENT PERSONNELS

1. Soumission de la demande

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

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.

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.

2. Réception de la demande

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.

2.2 La demande devra être traitée dans les soixante (60) jours suivant sa réception.

3. Vérification de l'identité

3.1 Avant de traiter la demande, l'identité de la personne 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.

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

4. Réponse aux demandes incomplètes ou excessives

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

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

5. Traitement de la demande

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

5.2 La personne responsable consulte les dossiers pertinents pour recueillir les renseignements personnels demandés, en veillant à respecter les restrictions légales éventuelles.

6. Examen des renseignements

6.1 Avant de communiquer les renseignements personnels à l'individu, la personne 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.

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

7. Communication des renseignements

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.

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.

8. Suivi et documentation

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.

8.2 Les détails de la demande, soit, les actions entreprises, les décisions prises et les dates correspondantes doivent être enregistrées dans un registre de suivi des demandes d'accès, incluant :

- 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).

9 Protection de la confidentialité

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.

10 Gestion des plaintes et des recours

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.

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

PROCÉDURE DE TRAITEMENT DES PLAINTES

1. Réception des plaintes

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

1.2 Le personnel doit informer immédiatement le service responsable de la réception des plaintes.

2. Évaluation préliminaire

2.1 La personne responsable désignée examine chaque plainte pour évaluer sa pertinence et sa gravité.

2.2 Les plaintes frivoles, diffamatoires ou sans fondement évident peuvent être rejetées. Toutefois, une justification doit être fournie au à la personne ayant déposé une plainte

3 Enquête et analyse

3.1 La personne responsable chargée de la gestion de la plainte mène une enquête approfondie en collectant des preuves, en interrogeant les parties concernées et en recueillant tous les documents pertinents.

3.2 La personne responsable doit être impartiale et avoir l'autorité nécessaire pour résoudre la plainte.

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

4 Résolution de la plainte

4.1 La personne responsable de la plainte propose des solutions appropriées pour résoudre la plainte dans les meilleurs délais.

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. Communication avec la personne ayant déposé une plainte

5.1 La personne responsable de la plainte communique régulièrement avec la personne ayant déposé une plainte pour la tenir informé de l'avancement de l'enquête et de la résolution de ladite plainte.

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

6 Clôture de la plainte

6.1 Une fois la plainte résolue, la personne responsable de la plainte doit fournir une réponse écrite à la personne ayant déposé une plainte, résumant les mesures prises et les solutions proposées.

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

Mars 2024 - Rédaction : l'équipe de Culture Lanaudière

1. Aperçu

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

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 clientèles.

3. Portée

Cette procédure s'applique à notre 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 clientèles.

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. Procédures

5.1 Réception des demandes

5.1.1 Les demandes de désindexation et de suppression des renseignements personnels doivent être reçues par la personne responsable désignée.

5.1.2 Les personnes peuvent soumettre leurs demandes par le biais de canaux spécifiques tels que le formulaire en ligne, l'adresse courriel dédiée;

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;

5.2.2 Cela peut être fait 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, Culture Lanaudière peut refuser de donner suite à la demande.

5.3 Évaluation des demandes

5.3.1 La personne 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 Il existe aussi des raisons parfaitement valables pour lesquelles Culture Lanaudière pourrait 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.

5.5 Désindexation ou suppression des renseignements personnels

5.5.1 La personne 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 La personne responsable est chargée de communiquer avec celles qui ont déposé une demande 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 à la personne ayant déposé une demande 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.

1. Aperçu

Un plan d'intervention est essentiel pour gérer des cybers incidents 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 l'organisation est prête à intervenir en cas de cyber incident 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 (clients, partenaires, employés, sous-traitants, fournisseurs) qui accèdent à ces systèmes.

4. Reconnaître un cyber incident

Un incident de cyber sécurité 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 (compte d'utilisateur) inactif;
2. Accès distant excessif ou inhabituel concernant 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.

5. Coordonnées des personnes-ressources

Responsable de la protection des renseignements personnels
Andrée St-Georges, directrice générale
→ 450 753-7444 poste 25
→ andree.saint-georges@culturelanaudiere.qc.ca

Responsable de la cyber sécurité
Maude Desjardins, Agente de développement culturel numérique
→ 450 753-7444 poste 24
→ adn@culturelanaudiere.qc.ca

Responsable des données sensibles en ligne
Guillaume Payette-Brisson, Agent web
→ 450 753-7444 poste 26
→ soutien@culturelanaudiere.qc.ca

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 :

A. Compléter le registre d'incidents de confidentialité pour documenter l'incident;

B. 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 autorisés, d'une divulgation non autorisée ou de toute atteinte 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.

C. Et, le signaler également aux personnes dont les renseignements personnels sont visés par l'incident.

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 :

A. Déconnecter immédiatement du réseau les appareils visés par un rançongiciel;
B. Ne RIEN EFFACER sur de vos appareils (ordinateurs, serveurs, etc.);
C. Examiner le rançongiciel et déterminer comment il a infecté l'appareil. Cela vous aidera à comprendre comment l'éliminer;
D. Communiquer avec les autorités locales pour signaler l'incident et coopérer à l'enquête;
E. 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.
F. 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.
G. 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.**
H. 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).
I. Protéger les systèmes pour éviter toute nouvelle infection en mettant en œuvre des correctifs ou des rustines pour empêcher toute nouvelle attaque.

8. Piratage d'un compte – Intervention spécifique

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

A. Aviser nos clientèles et 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;
B. Vérifier si on a encore accès au compte en ligne. Sinon, communiquer avec le support de la plateforme pour tenter de récupérer l'accès;
C. Changer le mot de passe utilisé pour se connecter à la plateforme;
D. Si le mot de passe est réutilisé ailleurs, changer également tous ces mots de passe;

E. Activer le double facteur d’authentification pour la plateforme;
F. Supprimer les connexions et les appareils non légitimes de l’historique de connexion.

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 :

A. 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.
B. 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.
C. 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.

1. Aperçu

Le départ d'un 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.

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 Culture Lanaudière 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 la personne;
4.1.2 Désactiver l'accès de la personne à tous les systèmes. Suivre la liste des rôles et des accès.
4.1.3 Supprimer les données professionnelles des appareils appartenant à cette personne :

- 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).

4.1.4 S'assurer que la personne 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 la personne 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 Idéalement, ne jamais supprimer le compte courriel d’un employé. La bonne pratique serait de créer une boîte courriel partagée et de bloquer les accès tel que mentionné plus bas.
4.3.2 Modifier le mot de passe du compte dans le système de courriels de Culture Lanaudière. Passer en revue la section 4.4 Accès au réseau et au Cloud avant de réactiver le compte.
4.3.3 Si la personne 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;
4.3.4 Créer un message d'absence pour le compte de messagerie conformément aux directives de communication de Culture Lanaudière;
4.3.5 Supprimer le nom de la personne des listes de diffusion de courriels internes;
4.3.6 Supprimer le nom de la personne 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 fournisseurs avec lesquels la personne 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 la personne. 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.

4.4 Accès au réseau et/ou au Cloud
4.4.1 Supprimer le nom de la personne 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 Culture Lanaudière vers un emplacement central;
4.4.3 Révoquer l'accès de la personne au compte infonuagique de Culture Lanaudière;
4.4.4 Supprimer les fichiers de travail de tout compte de stockage personnel.

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

4.4.6 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'ordinate