POLITIQUE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS

Table des matières

1. Objectifs & Portée

L'hôtel Universel de Rivière-du-Loup est assujetti à la Loi sur la protection des renseignements personnels dans le secteur privé, la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (Loi 25) et la Loi sur le cadre juridique des technologies de l'information

Les objectifs généraux de cette politique sont :

- D'assurer la conformité aux obligations de la législation applicable en matière de protection des renseignements personnels;
- De protéger les droits du personnel, des clients, et des partenaires potentiels et existants;
- D'intégrer les bonnes pratiques de protection des renseignements personnels dans les processus et procédures pour les renseignements personnels qui sont collectées, déclarées, générées et traitées dans le cadre des opérations normales de L'Hôtel Universel de Rivière-du-Loup;
- De se prémunir d'un risque de brèche de données.

2. Rôles et responsabilités

Les principales parties prenantes de la sécurité de l'information de L'Hôtel Universel de Rivière-du-Loup et leurs responsabilités respectives en matière de protection des informations sont décrites ci-dessous.

- **Direction générale ou Président**
  - Ultimement responsable du respect de cette politique.
  - Nommer un responsable de la protection des renseignements personnels
  - Fournir les ressources nécessaires, s'assurer que les personnes ayant les compétences appropriées sont en place et promouvoir la sensibilisation en général et de cette politique.
- **Responsable des renseignements personnels**
  - Consigner tout incident de confidentialité lui étant rapporté dans un registre
  - Signaler toutes les brèches de données ou l'exposition accidentelle des données personnelles au public et à la Commission d'accès à l'information (CAI).
  - Comprendre les lois applicables en matière de protection des renseignements personnels, ainsi que la manière de les appliquer à L'Hôtel Universel de Rivière-du-Loup.
  - Fournir des conseils aux différents intervenants.
  - Sensibiliser les employés et participer aux mises à jour du cadre de sécurité de l'information de l'organisation.
  - Participer aux évaluations d'impact sur la vie privée.
  - S'assurer de conseiller la haute direction de L'Hôtel Universel de Rivière-du-Loup sur les mesures à mettre en place afin de s'assurer de la protection des droits à la vie privée de ses clients.
  - Responsable de la gestion des demandes d'accès à l'information.
  - Responsable de la gestion des plaintes concernant la protection des renseignements personnels

- **Ensemble des employés**
  - Suivre les politiques et procédures en matière de protection des renseignements personnels.
  - Participer activement au programme de formations de sensibilisation à la sécurité de l'information.
  - Signaler tout incident de confidentialité sans délai.

3. Portée

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

4. Définitions

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

Conservation : stockage sécurisé des renseignements personnels pendant la durée requise.

Destruction : suppression, élimination ou effacement définitif des renseignements personnels.

Anonymisation : processus de modification des renseignements personnels de manière à ne plus permettre en tout temps et de façon irréversible l'identification, directe ou indirecte, des individus concernés.

5. Procédure

5.1 Durée de conservation

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

- renseignements concernant les employés de l'entreprise,

- renseignements concernant les membres du conseil d'administration,

- renseignements concernant la clientèle de l'entreprise,

- renseignements concernant les candidats.

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

- Employés de l'entreprise : 7 ans après la fin d'emploi.
- Les candidatures reçues : 2 ans après la réception de la candidature
- Membres du C.A. : 7 ans après la fin du mandat.
- Clients : variable en fonction du type de renseignement personnel.

Pour plus de détails concernant l'ensemble des catégories établit, veuillez-vous référer à l'inventaire complet des renseignements personnels détenus.

5.2 Méthodes de stockage sécurisé

5.2.1 Les renseignements personnels se trouvent aux endroits suivants : Support papier, serveur informatique de l'organisation, support informatique, cloud, serveurs externes.

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

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

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

5.3 Destruction des renseignements personnels

5.3.1 Pour les renseignements personnels sur papier, ceux-ci seront totalement déchiquetés.

5.3.2 Pour les renseignements personnels numériques, ceux-ci seront totalement supprimés des appareils (ordinateurs, téléphone, tablette, disque dur externe), des serveurs et des outils infonuagiques.

5.3.3 Un calendrier de destruction en fonction de la durée de conservation établie pour chaque catégorie de renseignements personnels a été fait et les dates destruction prévues.

5.3.4 La destruction des renseignements est réalisée de manière à ce que les renseignements personnels ne puissent pas être récupérés ou reconstitués.

5.4 Anonymisation des renseignements personnels

5.4.1 L'anonymisation des renseignements personnels sera effectué si l'organisation souhaite les conserver et les utiliser à des fins sérieuses et légitimes.

5.4.2 La méthode d'anonymisation des renseignements personnels choisit sera déterminée ultérieurement lorsque le Gouvernement du Québec adoptera un règlement à cet effet stipulant les critères et modalités nécessaires.

5.4.3 L'information conservée ne permettra plus, de manière irréversible, l'identification directe ou indirecte des individus concernés et une analyse régulière du risque de réidentification des données anonymisées en effectuant des tests et des analyses pour garantir leur efficacité sera effectué.

5.5 Formation et sensibilisation du personnel

5.5.1 Une 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 sera offerte aux employés concernés.

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

6. Principes directeurs de la protection des renseignements personnels

1. L'Hôtel Universel de Rivière-du-Loup et Les Entreprises Quéloup inc. sont responsables des renseignements personnels dont elle possèdent la gestion.
2. Les fins auxquelles des renseignements personnels sont recueillis doivent être déterminées avant la collecte ou au moment de celle-ci.
3. Tout individu doit être informé de toute collecte, utilisation ou communication de renseignements personnels qui le concerne et y consentir, à moins qu'il ne soit pas approprié de le faire.
4. L'Hôtel Universel de Rivière-du-Loup et Les Entreprises Quéloup inc. ne peuvent recueillir que les renseignements personnels nécessaires aux fins déterminées et doit procéder de façon honnête et transparente.
5. À moins que la personne concernée n'y consente ou que la loi ne l'exige, les renseignements personnels ne doivent être utilisés ou communiqués qu'aux fins auxquelles ils ont été recueillis. L'Hôtel Universel de Rivière-du-Loup et Les Entreprises Quéloup inc. ne doivent conserver les renseignements personnels qu'aussi longtemps que cela est nécessaire pour répondre à ces fins.
6. Les renseignements personnels doivent être aussi exacts, complets et à jour que possible afin de satisfaire aux fins auxquelles ils sont destinés.
7. Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité.
8. Les renseignements précis sur ses politiques et les pratiques concernant la gestion des renseignements personnels sont facilement accessibles au public.

9. L'Hôtel Universel de Rivière-du-Loup et Les Entreprises Quéloup inc. Informeront toute personne qui en fait la demande de l'existence de renseignements personnels qui la concernent, de l'usage qui en est fait et du fait qu'ils ont été communiqués à des tierces parties, et lui permettra de les consulter. Il sera aussi possible de contester l'exactitude et l'intégralité des renseignements et d'y faire apporter les corrections appropriées.
10. Toute personne doit être en mesure de se plaindre du non-respect par une organisation des principes énoncés ci-dessus. La plainte doit être adressée au responsable de la protection des renseignements personnels de L'Hôtel Universel de Rivière-du-Loup et des Entreprises Quéloup inc.

7. Responsabilité

- L'Hôtel Universel de Rivière-du-Loup et Les Entreprises Quéloup inc. sont responsables du respect de tous les principes de protection des renseignements personnels et en mesure de le démontrer.
- Les modifications aux lois qui ont un impact direct ou indirect sur le programme de protection des renseignements personnels de L'Hôtel Universel de Rivière-du-Loup et des Entreprises Quéloup inc. seront appliquées le plus tôt possible.
- L'Hôtel Universel de Rivière-du-Loup et Les Entreprises Quéloup inc. ont procédé à la nomination d'une personne responsable du respect des lois applicables en matière de protection des renseignements personnels. Les coordonnées de la personne nommée sont publiées sur les sites web pertinents.
- L'Hôtel Universel de Rivière-du-Loup et Les Entreprises Quéloup inc doivent utiliser et maintenir les systèmes et outils technologiques appropriés pour assurer la confidentialité des données de ses employés et citoyens.
- L'Hôtel Universel de Rivière-du-Loup et Les Entreprises Quéloup inc. doivent documenter et gérer les risques en matière de protection des renseignements personnels.
- L'Hôtel Universel de Rivière-du-Loup et Les Entreprises Quéloup inc doivent veiller à ce que le personnel pertinent reçoive une formation sur la protection des données pour les aider à comprendre leurs responsabilités lors du traitement des données personnelles.
- L'Hôtel Universel de Rivière-du-Loup et Les Entreprises Quéloup inc doivent procéder à une évaluation des facteurs relatifs à la vie privée 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 ainsi que pour tout transfert hors Québec.

8. Consentement et traitement des données

- L'Hôtel Universel de Rivière-du-Loup et Les Entreprises Quéloup inc publient sur ses sites web un avis de confidentialité à jour, précis et facilement accessible. L'avis explique de manière simple quelles données sont recueillies et comment elles sont utilisées.
- Le consentement doit être manifeste, libre, éclairé et être donné à des fins spécifiques. Il est demandé à chacune de ces fins, en termes explicites, simples et clairs.
- L'Hôtel Universel de Rivière-du-Loup et Les Entreprises Quéloup inc. veillent à ce que toutes les données personnelles soient traitées de manière juste et transparente.
- L'Hôtel Universel de Rivière-du-Loup et Les Entreprises Quéloup inc s'assurent que les données personnelles ne sont pas utilisées, extraites ou réutilisées de manière opportuniste autrement

que de la manière déclarée aux clients et visiteurs dans l'avis de confidentialité accessible au public sur les sites web et aux employés dans le manuel de l'employé et/ou la politique d'utilisation acceptable.

- L'Hôtel Universel de Rivière-du-Loup et Les Entreprises Quéloup inc veillent à ce que seul le personnel ayant un besoin de savoir ait accès aux données personnelles contrôlées ou traitées par l'organisation.
- L'Hôtel Universel de Rivière-du-Loup et Les Entreprises Quéloup inc s'assurent que les exigences de conservation des données sont respectées et que la conservation des données personnelles est réduite au minimum, conformément aux lois applicables.
- L'Hôtel Universel de Rivière-du-Loup et Les Entreprises Quéloup inc préconisent une approche de 'Privacy by Design' pour tous les nouveaux projets, systèmes ou processus afin qu'ils soient conçus avec la protection des données à l'esprit dès le départ
- Les acquisitions de données et les flux de traitement de L'Hôtel Universel de Rivière-du-Loup et Les Entreprises Quéloup inc sont compris, documentés et maintenus. Un inventaire des renseignements personnels est maintenu à jour.

9. Divulgation des données

- Les données personnelles acquises, conservées et/ou traitées par L'Hôtel Universel de Rivière-du-Loup et Les Entreprises Quéloup inc ne sont pas partagées sans objectif prédéfini, ou sans que cela ne représente une exception prévue dans la loi.
- Les données personnelles gérées par L'Hôtel Universel de Rivière-du-Loup et des Entreprises Quéloup inc ne doivent pas être partagées de manière informelle, que ce soit à l'interne ou à l'externe.
- L'approbation du responsable de la protection des renseignements personnels est requise lorsque des données personnelles doivent être partagées.

10. Externalisation des données à des tierces parties

- Une liste de tous les tierces parties impliqués dans la collecte et le traitement des données est conservée.
- Les services fournis sont documentés dans la liste, y compris l'objectif du partage de données.
- Des ententes de traitement sont en place. Ces ententes définissent les obligations et les responsabilités de chacune des parties.
- Une vérification de diligence raisonnable en matière des risques liées à la protection des renseignements personnels et de sécurité est effectuée avant que de nouvelles tierces parties ne soient engagées.
- Les emplacements de traitement de données effectués par les tierces parties sont connus et documentés.
- Les évaluations concernant le pays et/ou des juridictions sont effectuées avant que le traitement des données personnelles ne soit externalisé.

11. Transfert de données hors Québec

- L'Hôtel Universel de Rivière-du-Loup et Les Entreprises Quéloup inc mettent tout en place pour limiter les flux de données personnelles hors Québec.

12. Droits des individus

- L'Hôtel Universel de Rivière-du-Loup et Les Entreprises Quéloup inc respectent les droits des individus concernant la protection des renseignements personnels dans les limites des lois et réglementations. Ils ont le droit:
  - D'être informé du traitement de leurs données personnelles.
  - De savoir comment, quand et pourquoi leurs données personnelles sont partagées
  - D'avoir accès à leurs données.
  - D'être oubliés.
  - De pouvoir recevoir une copie de leurs données personnelles.
  - De refuser des services tels que la prise de décision automatisée, de recevoir des chaînes de courriels, et autres messages électroniques.
  - De faire rectifier leurs données si elles sont inexactes.
  - De limiter le traitement de leurs données.
  - De se voir demander le consentement lorsque des données personnelles sont divulguées ou demandées à des tierces parties si elles ne sont pas clairement exemptées par la loi.
- L'Hôtel Universel de Rivière-du-Loup et Les Entreprises Quéloup inc doivent s'assurer que les personnes sont conscientes que leurs données sont traitées et qu'elles comprennent comment elles peuvent exercer leurs droits.
- L'Hôtel Universel de Rivière-du-Loup et Les Entreprises Quéloup inc assureront la récupération, la correction ou la suppression des données suivant la réception d'une demande. Elle pourrait refuser une demande avec justification ou dans les limites de la Loi.
- Une documentation des demandes et des plaintes sera maintenue.

13. Gestion des incidents

13.1 Déclaration d'incident de confidentialité lié aux renseignements personnels

- L'Hôtel Universel de Rivière-du-Loup et Les Entreprises Quéloup inc veillent à ce que les exigences applicables en matière de signalement de brèche de renseignements personnels soient respectées dès la découverte de la brèche.
- Un registre d'incident de confidentialité est établi, documenté, maintenu et mis à disposition de la CAI, sur demande.
- L'Hôtel Universel de Rivière-du-Loup et Les Entreprises Quéloup inc veilleront à appliquer immédiatement des mesures raisonnables de confinement de la situation ou des correctifs.
- L'Hôtel Universel de Rivière-du-Loup et Les Entreprises Quéloup inc effectueront une analyse de préjudice sérieux de tout incident lié à des renseignements personnels afin de déterminer si une notification officielle à la CAI, à un individu ou à une autre autorité est requise.

13.2 Réponse aux incidents

- L'Hôtel Universel de Rivière-du-Loup et Les Entreprises Quéloup inc. établissent, documentent et tiennent à jour un plan de réponse aux incidents. Le plan prévoit la

gestion des incidents impliquant des renseignements personnels et est testé au moins aux deux ans.

14. Formation des employés

Un programme de formation sur les risques de cybersécurité qui inclut la couverture des risques liés à la protection des renseignements personnels est mis en place et révisé une fois par année.

15. Exceptions

L'Hôtel Universel de Rivière-du-Loup et Les Entreprises Quéloup inc sont conscientes que dans certaines circonstances, les lois sur la protection de la vie privée permettent que les données personnelles acquises soient divulguées sans le consentement de l'employé ou d'un individu:

- À des tierces parties dans certaines circonstances telles que définies et énoncées par les lois.
- Aux organismes d'application de la loi.
- À une personne à qui cette communication doit être faite en raison d'une situation d'urgence mettant en danger la vie, la santé ou la sécurité de la personne concernée.
- À une personne ou à un organisme lorsque des circonstances exceptionnelles le justifient;
- À une personne ou à un organisme si cette communication est nécessaire dans le cadre de la prestation d'un service à rendre à la personne concernée par un organisme public, notamment aux fins de l'identification de cette personne.

Dans ces circonstances, une divulguera des données demandées sera effectué.

16. Révision

La présente politique sera révisée aux deux ans, ou au besoin suivant des changements contractuels, légaux, ou contextuels.

17. Historique du document

Date	Version	Description du changement	Approbation
2023-08-02	1.0	Mise en place de la politique.	

Politique de confidentialité et informations complémentaires

Dernière mise à jour : 21 novembre 2023

18. Définition harmonisée d'un renseignement personnel

Dans le cadre de la présente politique et en vertu de la Loi sur la protection des renseignements personnels dans le secteur privé, un renseignement personnel est considéré comme étant un renseignement qui concerne une personne physique et permet de l'identifier.

Le renseignement personnel d'une personne doit être considérez dans son ensemble afin de déterminer si celui-ci permet de révéler l'identité de la personne concernée.

- Son nom;
- Son numéro d'assurance sociale;
- Son numéro de permis de conduire;
- Son numéro d'assurance maladie;
- Son adresse;
- Son numéro de téléphone
- Son numéro matricule;
- Son âge;
- Son genre;
- Sa race, sa nationalité ou son origine ethnique
- Sa religion
- Son état civil;
- Ses antécédents médicaux, scolaires ou professionnels
- Ses identifiants en ligne;
- Son numéro d'identification d'employé;
- Les informations bancaires ou de cartes de crédit;
- Les informations collectées permettant la vérification d'identité impliquant la biométrie;
- L'information permettant de géolocaliser une personne;
- S'ajoutent à la liste plusieurs éléments propres à son identité physique (dont la photographie), physiologie, génétique, psychique, santé, économique, culturelle ou sociale.

Informations qui ne sont pas considérées comme des renseignements personnels[1] :

- Les renseignements qui ne concernent pas directement un individu (ex. code postal)
- Les renseignements sur une entreprise
- Les renseignements anonymisés (dans la mesure qu'il est impossible de les relier à une personne identifiable)
- Les renseignements gouvernementaux

[1] Commissariat à la protection de la vie privée du Canada

Exception pour les renseignements considérés publics

Dans tous les cas, l'ensemble des renseignements personnels concernant un individu devrait être protégé, sauf certains renseignements considérés « publics ». Au sens de la Loi, « un renseignement personnel qui a un caractère public en vertu de la loi n'est soumis aux règles de protection des renseignements personnels prévues par le présent chapitre » (R.L.R.Q., c. A-2.1, a.55). Quelques exemples de renseignements personnels possédant un caractère public : le nom, le titre, la fonction, l'adresse et le numéro de téléphone du lieu de travail d'un membre d'un organisme public, de son conseil d'administration ou de son personnel de direction (R.L.R.Q., c A-2.1, a.57).

19. Protection des renseignements personnels – Rôles et responsabilités

Direction générale ou Président

- Ultimement responsable du respect de cette politique.
- Nommer un responsable de la protection des renseignements personnels
- Fournir les ressources nécessaires, s'assurer que les personnes ayant les compétences appropriées sont en place et promouvoir la sensibilisation en général et de cette politique.

Responsable des renseignements personnels

- Consigner tout incident de confidentialité lui étant rapporté dans un registre
- Signaler toutes les brèches de données ou l'exposition accidentelle des données personnelles au public et à la Commission d'accès à l'information (CAI).
- Comprendre les lois applicables en matière de protection des renseignements personnels, ainsi que la manière de les appliquer au Boréal Univers Gourmand.
- Fournir des conseils aux différents intervenants.
- Sensibiliser les employés et participer aux mises à jour du cadre de sécurité de l'information de l'organisation.
- Participer aux évaluations d'impact sur la vie privée.
- S'assurer de conseiller la haute direction du Boréal Univers Gourmand sur les mesures à mettre en place afin de s'assurer de la protection des droits à la vie privée de ses clients.
- Responsable de la gestion des demandes d'accès à l'information.
- Responsable de la gestion des plaintes concernant la protection des renseignements personnels

Politique de gestion des accès

20. Aperçu

L'élaboration et la mise en œuvre d'une politique de gestion des accès conformément à la Loi 25 revêt une importance cruciale pour assurer la sécurité des informations et la conformité légale au sein de l'organisation.

21. Objectif

Cette politique vise à définir les principes et les procédures pour la gestion des accès aux systèmes et aux informations personnelles contenus dans ces systèmes afin de garantir la confidentialité, l'intégrité et la disponibilité des données, tout en respectant les exigences légales de la Loi 25.

23. Responsabilités

a. Le responsable de la sécurité de l'information est chargé de la mise en œuvre de cette politique.

b. La haute direction et les directeurs de département sont responsables de l'attribution des droits d'accès conformément aux besoins opérationnels.

24. Identification et Authentification

Identification : Chaque utilisateur se voit attribuer un identifiant unique, généralement sous la forme d'un nom d'utilisateur, d'une adresse e-mail ou d'un identifiant spécifique à l'organisation. Cela garantit que chaque action est traçable jusqu'à un utilisateur spécifique.

Authentification : Les méthodes d'authentification doivent être robustes. Cela peut inclure l'utilisation de mots de passe forts, de méthodes de validation à deux facteurs, de cartes à puce ou de biométrie. Ces méthodes garantissent que seules les personnes autorisées peuvent accéder aux systèmes.

25. Attribution des Droits d'Accès

Attribution des droits : Les droits d'accès sont attribués en fonction des responsabilités professionnelles de chaque utilisateur. Cette mesure limite l'accès aux informations critiques uniquement à ceux qui en ont besoin pour effectuer leurs tâches. Les accès recensés sont inscrits dans le document d’inventaire des renseignements personnels.

Principe du Moindre Privilège : Cette approche garantit que chaque utilisateur détient uniquement les droits d'accès nécessaires à l'accomplissement de ses tâches. Ainsi, les risques liés à des autorisations excessives sont minimisés.

26. Surveillance des Accès

a. Les activités d'accès aux systèmes sont surveillées régulièrement.

b. Toute activité anormale sont signalée et examinée immédiatement.

27. Gestion des Privilèges

a. Les privilèges d'accès sont régulièrement révisés pour s'assurer de leur pertinence continue.

b. Les droits d'accès sont révoqués dès que l'utilisateur n'a plus besoin de les détenir.

28. Processus de Demande d'Accès

a. Tout nouvel accès est soumis à une demande formelle.

b. Les demandes sont soumises à un processus d'approbation où les responsables appropriés évaluent la nécessité de l'accès. L'accès n'est accordé qu'après une approbation formelle.

29. Gestion des Départs

Révocation immédiate : Lorsqu'un employé quitte l'organisation ou change de responsabilités, ses droits d'accès sont révoqués immédiatement. Cela réduit le risque de fuites de données ou d'accès non autorisés après le départ de l'employé. Veuillez-vous référez à la politique portant sur le roulement du personnel afin d'obtenir davantage d'information à ce sujet.

30. Formation et Sensibilisation

a. Les utilisateurs seront formés sur les bonnes pratiques de sécurité et sur la gestion appropriée de leurs droits d'accès.

b. Une sensibilisation continue à la sécurité de l'information sera assurée.

31. Conformité Légale

Mises à jour régulières : La politique est soumise à des révisions régulières pour s'aligner sur les évolutions de la Loi 25. Toute modification législative est intégrée immédiatement pour garantir la conformité continue.

Politique mise à jour le 22 novembre 2023

Procédure de demande de désindexation et de suppression des renseignements personnels

32. Aperçu

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

33. 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 clients.

34. 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 clients.

35. 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.

36. Procédure

36.1 Réception des demandes

5.1.1 Les demandes de désindexation et de suppression des renseignements personnels doivent être reçues par le responsable désigné.

5.1.2 Les clients doivent soumettre leurs demandes par courriel ou par la poste afin que celle-ci soit prise en charge par le responsable désigné.

36.2 Vérification de l'identité

36.2.1 Avant de traiter la demande, l'identité de l'individu doit être vérifiée de manière raisonnable par le responsable du traitement de la requête.

36.2.2 En l'absence de suffisamment d'éléments permettant d'identifier de manière satisfaisante le demandeur et de confirmer identité, l'organisation pourra refuser de donner suite à la demande.

36.3 Évaluation des demandes

36.3.1 Le responsable examinera attentivement les demandes et les renseignements personnels concernés afin de déterminer leur admissibilité à la désindexation ou à la suppression.

36.3.2 L'ensemble des demandes seront traitées de manière confidentielle et, en l'absence d'élément contraignant, dans le respect des délais prévus.

36.4 Raisons d'un refus

5.4.1 Il existe certaines raisons valables pour lesquelles une décision de refus de suppression ou de désindexation pourra être prise en regard des renseignements personnels identifiées dans une demande :

- Afin de permettre le rendu des biens et des services au client ;
- Afin de se conformer à des exigences contenues dans le droit du travail ;
- Pour des raisons juridiques en cas de litige.

36.5 Désindexation ou suppression des renseignements personnels

5.5.1 Le responsable ainsi que son équipe, s'il y a lieu, doivent prendre les mesures nécessaires pour désindexer ou supprimer les renseignements personnels conformément aux demandes admissibles.

36.6 Communication du suivi

36.6.1 Le responsable ainsi que son équipe, s'il y a lieu, communiquera avec les demandeurs au cours du processus, en fournissant des mises à jour sur l'état d'avancement du traitement des demandes admissibles.

36.6.2 Tout retard ou problème éventuel rencontré lors du traitement des demandes sera communiqué aux demandeurs dans les délais prescrits

36.7 Suivi et documentation

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

36.7.2 Les enregistrements incluront les détails des demandes, les mesures prises, les dates et les résultats des actions effectuées.

Dernière mise à jour : 22 novembre 2023

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

37. Aperçu

La création d'une procédure de gestion des incidents de sécurité et des violations des renseignements personnels est essentielle afin d'assurer une réponse rapide et efficace en cas de problématique.

38. Objectif

L'objectif de cette procédure est de garantir une réponse rapide, coordonnée et efficace en cas d'incident de sécurité ou de violation des renseignements personnels au sein de l'organisation.

39. 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.

40. Reconnaître un cyberincident

40.1 Identification de l'Incident

a. Toute personne ayant connaissance d'un incident de sécurité ou d'une violation des renseignements personnels doit le signaler immédiatement à la haute direction.

b. L'incident doit être documenté en détail, y compris la date, l'heure, la description de l'incident, les personnes impliquées et toute action immédiate prise.

Certains indicateurs sont susceptibles de laisser croire qu'un incident de sécurité a eu lieu.

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 dans votre 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.

40.2 Classification de l'Incident

a. L'équipe de gestion des incidents doit évaluer la gravité de l'incident en utilisant une échelle prédéfinie.

b. La classification doit guider la réponse appropriée en fonction de la nature et de l'étendue de l'incident.

40.3 Constitution de l'Équipe de Gestion des Incidents

a. Le responsable de la sécurité de l'information doit former une équipe de gestion des incidents comprenant des représentants de la sécurité, des technologies de l'information, des ressources humaines, des communications et des affaires juridiques.

b. 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.

41. Coordonnées des personnes-ressources

Rôle	Nom	Téléphone	Adresse de courriel
Responsable du traitement des incidents	Kéréon inc.		https://www.kereon.com/
Direction	Martin Lévesque		
Responsable des TI	Atria		https://www.atria-ti.com/
Responsable des communications	Martin Lévesque		
Avocat-conseil	À déterminer		
Assureur en cybersécurité	À déterminer		

42. 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 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.*
  - *Et, le signaler également aux personnes dont les renseignements personnels sont visés par l'incident.*

43. 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 de 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 (breach coach).*
- ☐ *Protéger les systèmes pour éviter toute nouvelle infection en mettant en œuvre des correctifs ou des rustines pour empêcher toute nouvelle attaque.*

44. 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 clients 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.*
- ☐ *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.*

45. 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.*

Dernière mise à jour : 22 novembre 2023

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

46. Objectif

La présente procédure a pour but de décrire les étapes essentielles du traitement d'une plainte relative au respect de la vie privée et la protection des renseignements personnels.

47. Cadre légal

La présente procédure s'interprète conformément aux obligations imposées à l'hôtel Universel de Rivière-du-Loup et aux Entreprises Quéloup inc. en vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* ou la *Loi sur la protection des renseignements personnels dans le secteur privé*.

48. Champ d'application

Cette procédure s'adresse au responsable de la protection des renseignements personnels et à la personne habilitée à agir en son absence.

49. Modification

Cette procédure sera révisée tous les deux ans et modifiée au besoin. Tout changement apporté aux normes, aux systèmes ou aux recommandations à la suite de vérifications ou d'incidents majeurs peut entraîner des changements à la présente procédure.

50. Principes directeurs

- Toutes plaintes doivent être accueillies et traitées adéquatement.
- Une plainte est une occasion d'améliorer la qualité des services offerts ainsi qu'assurer la conformité légale et réglementaire.
- Toute personne peut porter plainte à la personne désignée pour dénoncer une situation brimant sa vie privée ou la protection de ses renseignements personnels.

51. Personne désignée

- Le responsable de la protection des renseignements personnels s'assure de la réception et du traitement de la plainte ainsi que des communications avec le plaignant.
- Le responsable de la protection des renseignements personnels peut consulter le comité sur l'accès à l'information et la protection des renseignements personnels pour l'accompagner dans le traitement de la plainte.

52. Procédure de demande d'accès

52.1 Soumission de la demande

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

52.1.2 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.

52.1.3 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.

52.2 Réception de la demande

52.2.1 Une fois la demande reçue, un accusé de réception sera envoyé au demandeur afin de confirmer que sa demande a bel et bien été prise en compte.

52.2.2 La demande sera traitée dans les trente (30) jours suivant la remise de l'avis de réception et suivant le processus de vérification de l'identité du demandeur.

52.3 Vérification de l'identité

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

52.3.2 Dans le cas où l'identité du demandeur ne peut être vérifiée de manière satisfaisante, l'organisation se réserve le droit de refuser de divulguer les renseignements personnels demandés et ce, jusqu'à l'obtention des informations ou documents nécessaires permettant l'identification du demandeur.

52.4 Réponse aux demandes incomplètes ou excessives

52.4.1 Si une demande d'accès aux renseignements personnels est incomplète ou excessive, le responsable de la protection des renseignements personnels communiquera avec l'individu afin de demander des informations supplémentaires ou des clarifications à cet effet.

52.4.2 L'organisation se réserve le droit de refuser une demande si celle-ci juge qu'elle est manifestement abusive, excessive ou non justifiée.

52.5 Traitement de la demande

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

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

52.6 Examen des renseignements

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

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

52.7 Communication des renseignements

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

52.7.2 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.

52.8 Suivi et documentation

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

52.8.2 Les détails de la demande, les actions entreprises, les décisions prises et les dates correspondantes seront enregistrés dans le 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).

52.9 Protection de la confidentialité

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

52.10 Gestion des plaintes et des recours

52.10.1 Si la réponse obtenue ne satisfait pas le demandeur au terme du processus d'accès aux renseignements personnels, celui-ci pourra se prévaloir de recours à cet effet en contactant la Commission d’accès à l’information du Québec.

52.10.2 Les plaintes doivent être traitées conformément aux politiques et procédures internes en matière de gestion des plaintes indiqué ci-après.

53. Procédure de traitement des plaintes

53.1 Réception des plaintes

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

53.1.2 L'employé informe sur réception, le responsable de la réception de la plainte déposée.

53.2 Évaluation préliminaire

53.2.1 Le responsable désigné procède à l'examen de la plainte afin de déterminer sa pertinence et sa gravité.

53.2.2 Les plaintes frivoles, diffamatoires ou sans fondement évident pourront être rejetées le cas échéant et cette décision ainsi que les motifs soutenants celle-ci seront communiqué au plaintif.

53.3 Enquête et analyse

53.3.1 Le responsable chargé de la plainte procèdera à l'enquête en effectuant la collecte des preuves, en interrogeant les parties concernées, en recueillant tous les documents pertinents et en prenant toute mesures jugées nécessaires dans le cadre de l'enquête.

53.3.2 Le responsable maintiendra la confidentialité des informations liées à la plainte et veillera à ce que toutes les parties impliquées soient traitées équitablement.

53.4 Résolution de la plainte

53.4.1 Le responsable de la plainte propose des solutions appropriées afin de résoudre la plainte dans les meilleurs délais.

53.5 Communication avec le plaignant

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

53.6 Clôture de la plainte

53.6.1 Une fois la plainte résolue, le responsable de l'enquête fournira une réponse écrite au plaignant, résumant les mesures prises et les solutions proposées.

53.6.2 Toutes les informations et documents relatifs à la plainte seront conservés dans un dossier confidentiel.

Dernière mise à jour : 22 novembre 2023

Procédure de gestion du roulement du personnel

54. Aperçu

Le départ d'un membre du personnel peut entraîner des dommages intentionnels, accidentels ou une perte de données. La présente politique vise à contrôler davantage ces risques en mettant de l'avant les bonnes pratiques.

55. 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.

56. 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.

57. Procédure

57.1 Entrevue de départ ou mise à pied

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

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

57.1.3 Supprimer les données professionnelles des appareils appartenant aux employés :

- 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).

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

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

57.2 Téléphone

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

57.2.2 Changer le mot de passe de la messagerie vocale.

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

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

57.3 Accès aux courriels

57.3.1 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.

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

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

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

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

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

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

57.3.8 Désigner quelqu'un et lui donner les accès pour surveiller le courrier électronique de l'employé. 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.

57.4 Accès au réseau et/ou au Cloud

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

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

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

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

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

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

Dernière mise à jour : 22 novembre 2023