cie emploi laurentides Propulseur de potentiel humain

# POLITIQUE DE CONFIDENTIALITÉ DES DONNÉES

## PRÉAMBULE

ATTENDU QUE le Centre d'intégration en emploi Laurentides (CIE Laurentides) est un organisme privé à but non lucratif régie par la *Loi sur la protection des renseignements personnels dans le secteur privé* (RLRQ, chapitre P-39.1) ;

ATTENDU QUE dans le cadre de la prestation des services via ses différentes ententes, le CIE Laurentides doit procéder à la collecte, l'utilisation, la conservation et la destruction de renseignements personnels qui concernent les clients (individus et entreprises), les membres du personnel, les candidats à l'emploi, les membres de la corporation ainsi que ses administrateurs ;

ATTENDU QUE le CIE Laurentides recueille des renseignements personnels en application de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1).*

ATTENDU QUE de nouvelles dispositions législatives imposent au CIE Laurentides l'obligation d'adopter et de mettre en application des pratiques encadrant sa gouvernance des renseignements personnels afin d'assurer la protection de ceux-ci ;

ATTENDU QUE le non-respect de la loi peut engager la responsabilité des administrateurs et du personnel d'encadrement du CIE Laurentides par l'accomplissement d'un acte fautif ou par omission ;

Le Centre d'intégration en emploi Laurentides adopte la présente politique afin d'encadrer la protection des renseignements personnels.

## 1. Objectifs de la présente politique

Le CIE Laurentides a la volonté et l'obligation légale de se doter de pratiques sécuritaires afin d'assurer la confidentialité des informations personnelles que la corporation obtient, détient et utilise dans le cadre de la prestation de ses services. Ces pratiques incluent aussi la destruction des informations personnelles.

Par la présente politique, le Centre d'intégration en emploi Laurentides s'engage ainsi à protéger l'ensemble des renseignements personnels que son personnel utilise concernant les clients, les membres du personnel, les candidats à l'emploi, les membres de la corporation ainsi que ses administrateurs. La présente politique encadre aussi les demandes d'accès aux renseignements personnels ainsi que la rectification de ceux-ci.

## 2. La personne responsable

La directrice des communications et partenariats est désignée expressément par le conseil d'administration comme la personne responsable de l'accès aux informations personnelles et à la protection des renseignements personnels.

En ce sens, la directrice des communications et partenariats a pour fonction de veiller à assurer le respect et la mise en œuvre de la Loi sur la protection des renseignements personnels dans le secteur privé (RLRQ, chapitre P-39.1) et d'appliquer la présente politique.

Elle a également comme responsabilité de répondre aux demandes d'accès à l'information et de traiter ces demandes en conformité avec la Loi et la présente politique. Les coordonnées de la directrice des communications et partenariats sont les suivantes :

DIRECTRICE DES COMMUNICATIONS ET PARTENARIATS : Valérie Monette
COURRIEL : vmonette@cielaurentides.com
TÉLÉPHONE : 450 431-0028, poste 260

Si la directrice des communications et partenariats n'est pas disponible pour une période prolongée de plus de 30 jours et ne peut répondre à une demande d'accès à l'information, la directrice adjointe est désignée pour répondre et traiter la demande en son absence.

## 3. Demande d'informations sur les pratiques du CIE Laurentides en matière de protection des renseignements personnels

Les coordonnées de la directrice des communications et partenariats et son rôle en matière d'accès à l'information et de protection des renseignements personnels sont

affichés sur le site Internet du CIE Laurentides. La directrice des communications et partenariats a aussi l'obligation de rendre et maintenir accessible cette information par d'autres moyens qu'elle juge appropriés.

La directrice des communications et partenariats prête assistance à toute personne qui demande des informations concernant les pratiques et procédures encadrant la collecte et la protection des renseignements personnels incluant la durée de la détention de cette information.

## 4. Nature des renseignements personnels collectés, détenus et utilisés

Le CIE Laurentides, à titre de prestataire de ses différentes ententes de services, doit recueillir plusieurs renseignements personnels. Ces renseignements personnels sont consignés par écrit sur des formulaires ou des ententes, et ce, par le biais de divers moyens technologiques.

D'une manière non limitative, le CIE Laurentides doit recueillir des renseignements personnels afin de :

- Constituer un dossier concernant chaque client ;
- Compléter l'inscription des clients ;
- Compléter les notes reliées aux différentes rencontres ;
- Déterminer l'admissibilité du client ;
- Compléter le curriculum vitae des clients
- Constituer un dossier concernant les besoins particuliers des clients, le cas échéant ;
- Constituer les dossiers des employées ;
- Tenir un registre des membres de la personne morale et des administrateurs ;
- Faire parvenir l'infolettre mensuelle
- Autres fins nécessaires à la prestation de ses services.

### 4.1 Durée de conservation

La durée de conservation pour chacun des renseignements personnels collectés a été établit de la façon suivante :

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

- Membres (infolettre) : Variable en fonction du type de renseignement personnel

## 5. Consentement à la collecte et à l'utilisation des renseignements

Les clients, les membres du personnel, les candidats à l'emploi ainsi que les membres de la corporation et ses administrateurs ou toute autre personne qui fournit des renseignements personnels au CIE Laurentides doivent être informés et consentir par écrit à toute collecte de renseignements personnels les concernant, et ce, avant que ces données ne soient collectées et utilisées.

Le CIE Laurentides doit obtenir l'autorisation écrite de la personne concernée avant ou au moment de collecter des renseignements personnels sur celle-ci et avant de communiquer quelques renseignements personnels que ce soit à un tiers.

## 6. Règles de conservation des renseignements personnels (stockage et sécurité)

Les renseignements sont conservés à l'établissement principal de l'entreprise et dans la plateforme numérique LGESTAT qui se dote également d'une politique de confidentialité.

Le degré de sensibilité de chacun des lieux de stockage a été établi. Ces lieux de stockage, qu'ils soient papier ou numérique, sont adéquatement sécurisés.

La directrice des communications et partenariats s'engage à limiter l'accès et l'utilisation des renseignements personnels que le CIE Laurentides détient aux seules personnes détenant les fonctions appropriées au sein de l'entreprise, et ce, seulement lorsque ces renseignements sont nécessaires à l'exercice de leurs fonctions.

La directrice des communications et partenariats prend des mesures de sécurité propres à assurer la sécurité des renseignements compte tenu, notamment, de la sensibilité des renseignements, de leur finalité, de leur quantité et du support utilisé.

La directrice des communications et partenariats est responsable de la mise en place des mots de passe, de l'octroi des accès, et des diverses mesures informatiques, dont le système de sauvegarde « back-up » sécurisé.

La directrice des communications et partenariats s'assure que le CIE Laurentides ne recueille que les renseignements personnels nécessaires aux fins déterminées par Services Québec et ses différentes ententes.

## 7. Règles de destruction des renseignements personnels

Les renseignements personnels seront conservés qu'aussi longtemps que nécessaire pour la réalisation des finalités déterminées et conformément aux délais prescrits par la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1)* et ses règlements.

Il en est ainsi de toutes autres obligations législatives, dont celles à caractère fiscal et des renseignements personnels, des candidats rejetés dans le cadre des processus d'embauche.

À l'expiration de ces délais, la directrice des communications et partenariats s'assurera de la destruction des renseignements personnels contenus dans les dossiers, et ce, de manière sécuritaire.

### 7.1 Procédure de destruction

7.1.1 Les renseignements personnels sur papier seront totalement déchiqueté.
7.1.2 Les renseignements personnels numériques seront totalement supprimés des appareils (ordinateurs, téléphone, tablette, disque dur externe), des serveurs et des outils infonuagiques.
7.1.3 Un calendrier de destruction en fonction de la durée de conservation établie pour chaque catégorie de renseignements personnels sera être fait. Il est impératif de documenter les dates de destructions prévues.
7.1.4 La destruction sera réalisée de manière à ce que les renseignements personnels ne puissent pas être récupérés ou reconstitués.

## 8. Formation et sensibilisation du personnel

Une formation sur la procédure de conservation et de cybersécurité sera offerte à l'ensemble du personnel. Les membres du personnel seront également sensibilisés aux bonnes pratiques de sécurité des données et à l'importance du respect des procédures établies.

## 9. Les rôles et responsabilités des membres du personnel et des administrateurs

Les membres du personnel et les administrateurs de la personne morale peuvent avoir accès à des renseignements personnels sensibles dans le cadre de la gestion du CIE Laurentides, des relations du travail et de la prestation des différentes ententes.

Les membres du personnel et les administrateurs de la personne morale sont tenus à la discrétion sur ce dont ils ont connaissance à l'occasion de l'exercice de leurs fonctions et doivent respecter le caractère strictement confidentiel des renseignements personnels auxquels ils ont accès.

Chacun des membres du personnel, de la direction, des administrateurs, stagiaires et bénévoles s'engage personnellement à respecter la présente politique ainsi que les procédures qui y sont énoncées et à respecter le caractère hautement confidentiel des données auxquelles ils ont accès. Cette obligation perdure en tout temps, même après l'expiration du mandat ou la fin de l'emploi.

## 10. Règles de transmission à des tiers

Le CIE Laurentides ne peut transmettre à des tiers des renseignements personnels sauf lorsque ceux-ci sont autorisés par l'ensemble des parties.

La directrice des communications et partenariats s'assure que les renseignements personnels collectés ou les informations qui ont été portées à leur connaissance dans le cadre des activités de l'entreprise ne sont pas utilisés ou communiqués à des fins autres que celles pour lesquelles ils ont été recueillis ou obtenus, à moins que la personne concernée n'y consente ou que la Loi ne l'exige.

La transmission d'informations personnelles à des tiers pour des fins commerciales ou philanthropiques est interdite. En cas de réorganisation de la structure juridique du CIE Laurentides (fusion ou cession), les renseignements personnels font partie des actifs et peuvent être partagées sans consentement.

## 11. Exactitude des renseignements personnels

Les renseignements personnels qui sont collectés, détenus et utilisés doivent être exacts, complets et à jour. Toute personne peut faire une demande d'accès et de rectification des renseignements personnels la concernant, conformément à la Loi.

## 12. Accès aux renseignements personnels ou mise à jour des renseignements

Pour toute demande d'information ou de mise à jour concernant les renseignements personnels ou une demande d'information sur la présente politique, veuillez communiquer avec la directrice des communications et partenariats. Celle-ci procédera à l'évaluation de la demande.

La directrice des communications et partenariats, dans un délai de trente (30) jours et à la demande écrite de la personne concernée, confirmer ou infirmer l'existence d'un renseignement personnel la concernant et lui donner communication de ce renseignement en lui permettant d'en obtenir une copie, conformément à la *Loi sur la protection des renseignements personnels dans le secteur privé* (RLRQ, chapitre P-39.1).

### 12.1 Soumission de la demande

12.1.1 L'individu qui souhaite accéder à des 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.

12.1.2 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.

### 12.2 Réception de la demande

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

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

### 12.3 Vérification de l'identité et réponse aux demandes incompletes ou excessives

12.3.1 Avant de traiter la demande, l'identité de l'individu sera vérifiée de manière raisonnable. Si l'identité ne peut être vérifiée de manière satisfaisante, l'organisation peut refuser de divulguer les renseignements personnels demandés.

12.3.2 L'organisation se réserve le droit de refuser une demande si elle est manifestement abusive, excessive ou non justifiée.

12.4 Traitement de la demande

12.4.1 Une fois l'identité vérifiée, le responsable de la protection des renseignements personnels procèdera à la collecte des renseignements demandés afin de traiter la demande.

12.5 Examen des renseignements

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

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

12.6 Communication des renseignements

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

12.6.2 Les renseignements personnels seront communiqués à l'individu par voie électronique, par courriel postal sécurisé ou en personne, selon les préférences de l'individu et les mesures de sécurités appropriées.

12.7 Suivi et documentation

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

12.7.2 Les détails de la demande, les actions entreprises, les décisions prises et les dates correspondantes seront enregistré dans un registre de suivi des demandés d'accès.

13. Protection de la confidentialité

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

## 14. Incident de confidentialité

En cas d'accès, d'utilisation ou de communication non autorisés par la Loi ou par la personne concernée à un renseignement personnel ou la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement que le CIE Laurentides sur une ou des personne(s), la directrice des communications et partenaires doit :

- Suivre la procédure établit à l'interne en fonction de l'atteinte : rançongiciel, piratage ou perte/vol d'un appareil.
- Aviser la Commission d'accès à l'information (CAI) si nous sommes en présence d'un risque de préjudice sérieux;
- Aviser la personne visée par écrit;
- Prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent ;
- Aviser toute personne ou tout organisme susceptible de diminuer ce risque (obligation de conserver une preuve) ;
- Tenir un registre des incidents de confidentialité

## 15. Processus de traitement des plaintes

Conformément aux articles 42 à 44 de la *Loi sur la protection des renseignements personnels dans le secteur privé* (RLRQ, chapitre P-39.1), la personne qui est insatisfaite du traitement de sa demande d'accès à l'information ou de rectification peut demander la révision de cette décision auprès de la Commission d'accès à l'information, dans les 30 jours du refus de la demande ou de l'expiration du délai pour y répondre.

La demande doit être formulée par écrit et exposer brièvement les raisons de celle-ci en plus de payer les frais exigibles. Un formulaire de demande de révision est disponible sur le site internet de la Commission d'accès à l'information à l'adresse suivante :

https://www.cai.gouv.qc.ca/documents/CAI_FO_demande_revision_et_dexamen_mesentente.pdf

Pour toute autre insatisfaction quant à la collecte, l'utilisation ou la destruction des renseignements personnels détenus par le CIE Laurentides, une plainte peut être

formulée conformément à la politique de traitement de plaintes en vigueur au CIE Laurentides.

## 16. Gestion du roulement de personnel

Une politique est appliquée avant le départ d'un membre du personnel pour éviter les dommages intentionnels, accidentels ou la perte de données. Cette politique 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.

### 16.1 Entrevue de départ

16.1.1 Éteindre les ordinateurs et appareils professionnels de l'employé.
16.1.2 L'accès de l'employé à tous les systèmes sera désactivé.
16.1.3 Les données professionnelles seront supprimées des appareils appartenant aux employés :
- Observer l'utilisation supprimer les comptes de messagerie de son téléphone

16.1.4 L'employé retournera tout équipement appartenant à l'organisation : ordinateurs portables, tablettes, clés USB, etc.
16.1.5 Une liste de tous les emplacements où l'employé à stocké des donnes professionnelles, y compris les plateformes de stockage nuagique, sera compilée.

### 16.2 Téléphone

16.2.1 Le numéro de téléphone de l'employé ne sera pas transféré à un numéro externe, tel qu'un téléphone portable personnel ou via la téléphonie IP.
16.2.2 Le mot de passe de la messagerie vocale sera modifié.
16.2.3 Le message vocal sortant sera modifié conformément aux directives de communication.
16.2.4 Une personne de l'équipe sera désignée pour surveiller la messagerie vocale jusqu'à ce que ce numéro de téléphone puisse être supprimé ou réaffecté.

### 16.3 Accès aux courriels

16.3.1 Idéalement, ne jamais supprimer le compte courriel d'un employé. Créer une boîte courriel partagée et bloquer l'accès de l'employé.
16.3.2 Le mot de passe du compte dans le système de courriels de l'organisation sera modifié.

16.3.3 Si l'employé a utilisé un téléphone mobile personnel ou une tablette pour accéder à sa messagerie professionnelle, le compte de messagerie sera effacé ou supprimé.
16.3.4 Un message d'absence sera créé pour le compte de messagerie conformément aux directives de communication de l'organisation.
16.3.5 L'employé sera supprimé des listes de diffusion de courriels internes et des courriels spécialisés.
16.3.6 Les fournisseurs avec lesquels l'employé a travaillé seront contactés pour les informés du départ et leur fournir un nouveau contact.
16.3.7 Une personne à l'interne aura les accès pour surveiller le courrier électronique de l'employé. La boîte de courriels sera disponible trente (30) jours après le départ de l'employé après quoi le compte sera supprimé.

16.4 Accès aux réseaux

16.4.1 L'employé sera supprimé 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.
16.4.2 Tous les fichiers de travail qui ont pu être stockés en dehors des dossiers de sauvegarde principaux de l'organisation vers un emplacement central seront déplacés.
16.4.3 Les fichiers de travail de tout compte de stockage personnel seront supprimés.
16.4.4 Les règles d'accès pare-feu pour confirmer que l'utilisation ne dispose d'aucun autre accès, tel qu'un VPN direct depuis son pare-feu personnel à la maison seront passé en revue.
16.4.5 Confirmer qu'aucun logiciel d'accès à distance n'est installé sur les appareils (TeamViewer), que l'employé pourrait utiliser pour accéder à l'ordinateur ou au réseau.

Mise à jour: 22 septembre 2023