

## **POLITIQUE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS**

### **1. LES OBJECTIFS**

La présente politique constitue le cadre général concernant les comportements attendus des employés quant à la manipulation des données, l'accès aux données, l'utilisation des technologies de l'information, ainsi que les actions sur la gouvernance et la gestion des informations.

Cette politique souligne également l'importance d'assurer et préserver la confidentialité des renseignements personnels, le respect de la vie privée et la responsabilité éthique de toute personne qui détient des renseignements sur autrui.

De plus, elle indique les démarches et les principes généraux que les employés de Locweld doivent suivre afin d'accorder la plus haute importance aux informations sensibles dont ils ont accès, les démarches en matière de plaintes et incidents, ainsi que les actions nécessaires dans la prise en charge des exigences de sécurité de l'information.

### **2. LE CHAMP D'APPLICATION**

La présente politique s'applique à tous les employés de Locweld qui de manière directe ou indirecte ont accès aux données de clients, données personnelles des employés ou des candidats, ou autres données de l'entreprise définies comme sensibles par l'entreprise.

Tous les employés qui se trouvent dans les lieux de travail ou le télétravail, y compris les employés syndiqués, du bureau, les sous-traitants et les dirigeants sont impliqués dans la responsabilité de cette politique.

Le champ d'application est également appliqué sur les serveurs, bases de données et systèmes informatiques qui traitent ces données, y compris tout appareil régulièrement utilisé par courriels électroniques, l'accès au site Web ou d'autres tâches professionnelles. Tout utilisateur qui interagit avec les services informatiques de l'entreprise est également soumis à cette politique.

### **3. DÉFINITIONS ET CONCEPTS**

- **Confidentialité:** une exigence en vertu de laquelle une information est divulguée, traitée et mise à la disposition des seules personnes ou entités autorisées, selon les modalités établies.
- **Droit d'accès:** le droit d'utiliser un actif informationnel selon des modalités qui varient en fonction du niveau de privilège accordé.
- **Incident de sécurité informatique:** tout événement susceptible de contrevenir aux objectifs et aux normes institutionnelles de sécurité informatique.
- **Utilisatrice, utilisateur:** l'ensemble des employés de Locweld et toute personne physique ou morale appelée à utiliser les actifs informationnels autorisés par la haute direction.

## **POLITIQUE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS**

- **Authentifiant personnel:** une caractéristique exclusive, une information unique et confidentielle ou un objet unique détenu par l'employé, permettant de vérifier l'identité de cette personne. Il s'agit d'un mot de passe ou un numéro d'identification personnel prédéfinie et informé uniquement à l'utilisateur.
- **Adresse électronique:** Toute adresse utilisée relativement à l'un des comptes suivants :
  - un compte courriel Locweld;
  - un compte messagerie instantanée à de fins spécifiques ;
- **Actif informationnel:** tout équipement relié ou non au réseau, logiciel, système, donnée ou information utilisée pour l'hébergement, le traitement, la diffusion et l'échange d'information. Les actifs informationnels couvrent également les équipements, logiciels, systèmes, données ou informations qui lui appartiennent et ceux qui utilisent ou hébergent des actifs dont l'entreprise est propriétaire, fiduciaire ou dépositaire.
- **Activité commerciale:** Toute activité régulière ainsi que tout acte isolé qui revêtent un caractère commercial.
- **Coordonnées d'affaires:** Tout renseignement permettant d'entrer en contact ou de faciliter la prise de contact avec un individu dans le cadre de son emploi, de son entreprise ou de sa profession, tel que son nom, son poste ou son titre, l'adresse ou les numéros de téléphone ou de télécopieur de son lieu de travail ou son adresse électronique au travail.
- **Document:** Tous éléments d'information, quels que soient leur forme et leur support, notamment correspondance, note, livre, plan, carte, dessin, diagramme, illustration ou graphique, photographie, film, microforme, enregistrement sonore ou toute reproduction de ces éléments d'information
- **Renseignements personnels:** Tout renseignement concernant un individu identifiable, à savoir :
  - la race, la nationalité ou l'origine ethnique.
  - la religion;
  - l'âge ou l'état civil;
  - les transactions financières;
  - les numéros permettant d'identifier la personne (p. ex. numéro d'assurance sociale ou numéro de permis de conduire).
- **Renseignements personnels sur la santé:** En ce qui concerne un individu vivant ou décédé :
  - tout renseignement ayant trait à sa santé physique ou mentale.
  - tout renseignement relatif aux dons de parties du corps ou de substances corporelles faits par lui, ou tout renseignement provenant des résultats de tests ou d'examen effectués sur une partie du corps ou une substance corporelle de celui-ci.

**Remarque :** Ce qui n'est généralement pas considéré comme des renseignements personnels peut inclure :

## **POLITIQUE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS**

- Des renseignements qui ne concernent pas un individu, soit parce que le lien avec cette personne est trop vague ou trop distant (p. ex. un code postal s'applique à un vaste secteur où se trouve de nombreuses résidences).
  - Des renseignements anonymisés, pourvu qu'il ne soit pas possible de les relier à une personne identifiable.
  - Certains renseignements sur des employés comme leur nom et le titre du poste qu'ils occupent.
  - Les coordonnées d'affaires d'une personne qu'une organisation recueille, utilise ou communique uniquement pour entrer en contact avec elle dans le cadre de son emploi, de son entreprise ou de sa profession.
- **Dépersonnalisation et anonymisation des renseignements**  
Un renseignement personnel est « dépersonnalisé » lorsque ce renseignement « ne permet pas d'identifier directement la personne concernée ». Un renseignement concernant une personne physique est « anonymisé » lorsqu'il « ne permet pas, de façon irréversible, d'identifier directement ou indirectement cette personne ».

### **4. RAPPEL DU CADRE NORMATIF**

Cette politique est fondée sur la loi sur la PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LE SECTEUR PRIVÉ (LPRP), chapitre P-39.1 ainsi que la loi 25, LOI MODERNISANT DES DISPOSITIONS LÉGISLATIVES EN MATIÈRE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS, *ainsi que la* Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) du Canada.

### **5. CONTRÔLE D'ACCÈS**

Les accès aux données de Locweld sont définis selon le poste, les responsabilités et les permissions données par la haute direction. La gestion des accès existe pour assurer que les utilisateurs ne peuvent accéder qu'aux ressources dont ils ont besoin pour effectuer leur travail.

#### **5.1. Accès informatique:**

1. Chaque utilisateur sera identifié par un ID utilisateur unique, afin que chacun puisse être tenu responsable de ses actions.
2. L'utilisation des identités partagées n'est autorisée que là où elles sont appropriées, par exemple l'équipe des Inspecteurs.
3. Les enregistrements des accès des utilisateurs peuvent être utilisés comme éléments probants dans le cadre d'une enquête sur incident de sécurité.

## **POLITIQUE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS**

### **5.2. Responsabilités des utilisateurs:**

1. Tous les utilisateurs doivent verrouiller leur écran chaque fois qu'ils quittent leur bureau, pour réduire le risque d'accès non autorisé.
2. Tous les utilisateurs doivent veiller à ne laisser aucune information sensible ou confidentielle autour de leur poste de travail.
3. Tous les utilisateurs doivent tenir leurs mots de passe confidentiels et ne pas les partager.

### **5.3. Accès aux documents physiques (dossier des employés) :**

1. Tous les employés ont un dossier relatif à son parcours professionnel. Ce dossier est constitué par plusieurs documents dont la majorité est considérée comme strictement confidentiel. Afin de préserver le droit à la vie privée de l'employé, seules les personnes dûment autorisées, étant donné leurs fonctions professionnelles, peuvent consulter les documents pertinents contenus aux dossiers des employés.
2. Il y est interdit d'avoir accès à ces dossiers, toute personne au sein de l'entreprise pour qui la consultation du dossier n'est pas nécessaire à l'exercice de ses fonctions et de ses responsabilités.
3. *Il est permis à l'employé de consulter son dossier si l'autorisation est précisée à l'intérieur de la convention collective ou en vertu des règles prévues à la Loi sur la protection des renseignements personnels dans le secteur privé. A cet effet, l'employé doit faire la demande aux RH et la consultation sera faite dans un bureau réservé à cette fin et avec la présence d'un membre de l'équipe des Ressources Humaines.*

## **6. ACCÈS AUX INFORMATIONS CONFIDENTIELLES ET RESTREINTES**

L'accès aux données classées comme « confidentielles » ou « restreintes » quel qu'en soit sa forme ou son contenu, doit être limité aux personnes autorisées dont les responsabilités professionnelles l'exigent, tel que déterminé par la direction ou par une procédure prévue à cette fin.

## **7. COMMISSION D'ACCÈS À L'INFORMATION ET GESTION D'INCIDENT DE CONFIDENTIALITÉ**

En tenant compte de l'importance de cette politique pour la protection des renseignements sensibles et personnel, et pour la sécurité des données de l'entreprise, **un comité d'intervention** a été établi pour créer la relation avec la commission d'accès à l'information, pour assurer la mise en place des procédures et les démarches en cas d'un incident de confidentialité se produit.

Le comité d'intervention à l'information est composé de la façon suivante :

## **POLITIQUE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS**

### **Responsable du comité et de la protection de données (PRP):**

Pierre Lavoie (Président de Locweld)  
Tel : 450-659-9661  
[info@locweld.com](mailto:info@locweld.com)

**Équipe / members:** Chef des Opérations  
Directeur de TI  
Coordonatrice des RH  
Contrôleure

### **7.1. Responsabilités du responsable de la PRP :**

- Approuver les politiques et pratiques en matière de renseignements personnels que Locweld a établi;
- Participer au comité et gérer les actions nécessaires à la protection des renseignements personnels;
- Prend part à l'analyse des répercussions sur la confidentialité et l'évaluation du préjudice causé par un incident de confidentialité;
- Définir les communications nécessaires et l'engagement des membres du comité afin d'assurer l'application de cette politique.

### **7.2. Responsabilités du comité d'intervention à l'information:**

- Se rencontrer occasionnellement afin de tenir à jour cette politique.
- Définir les mesures à prendre en cas de besoin d'amélioration des procédures.
- Considérer la sensibilité du renseignement concerné, les conséquences appréhendées de son utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables.
- Assurer que les demandes de renseignements personnels sont utilisées aux fins d'utilisation prévues. « Un renseignement personnel ne peut être utilisé au sein de l'entreprise qu'aux fins pour lesquelles il a été recueilli, à moins du consentement de la personne concernée (art.110 alinéa 12, LPRDE) ».
- En cas d'incident, prendre les mesures nécessaires pour faire cesser les risques et dommages.
- Tenir un registre des incidents de confidentialité et mettre en évidence les mesures prises pour éviter que de nouveaux incidents similaires ne se produisent.

### **7.3. Incident de confidentialité:**

Pour l'application de la loi, un incident de confidentialité est :

- L'accès non autorisé par la loi à un renseignement personnel.
- L'utilisation non autorisée par la loi d'un renseignement personnel.
- La communication non autorisée par la loi d'un renseignement personnel.
- La perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement pouvant causer un préjudice.

## **POLITIQUE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS**

### **7.4. Procédure au cas d'un incident:**

Les incidents de confidentialité ou toute atteinte aux renseignements personnels qui sont à la possession d'une organisation doivent obligatoirement être déclarés à la Commission d'accès à l'information (CAI).

Le comité d'intervention procédera à un examen approfondi de la situation et émettra un rapport contenant les détails de l'incident et les mesures nécessaires pour mettre fin à la fuite de données. Des mesures pour éviter la répétition des incidents seront ensuite déterminées par le responsable du comité.

Le président du comité se responsabilise de faire la signalisation en temps opportun de tout incident de confidentialité à la Commission d'accès à l'information (CAI).

## **8. LA GOUVERNANCE DES DONNÉES**

### **8.1. Consentement d'utilisation des données**

Les fins pour lesquelles les renseignements personnels sont recueillis et les méthodes employées pour les recueillir sont énoncées ci-après afin d'assurer la transparence de la collecte et de répondre aux demandes d'information. Lors de la collecte de renseignements personnels :

- Un consentement doit être demandé, en termes simples et clairs, pour chacune des fins pour lesquelles les renseignements sont recueillis.
- Un consentement écrit doit être obtenu distinctement de toute autre information communiquée à un particulier.
- Les moyens de collecte doivent être clairement définis.
- La possibilité que les renseignements soient communiqués à l'extérieur du Québec doit être clairement signifiée, le cas échéant.

### **8.2. Exceptions relatives au consentement:**

La loi 25 prévoit qu'un organisme peut utiliser un renseignement personnel à une autre fin sans avoir à obtenir le consentement de la personne concernée dans les seuls cas suivants :

- Lorsque son utilisation est à des fins compatibles avec celles pour lesquelles il a été recueilli et qu'elle sert la personne concernée;
- Lorsque le renseignement personnel est nécessaire pour conclure une transaction commerciale;
- Lorsque le renseignement personnel est utilisé à des fins de recherche ou de production de statistiques;
- Lorsque le renseignement personnel est de nature commerciale (nom, titre, fonctions, adresse d'entreprise, adresse courriel et numéro de téléphone);

## **POLITIQUE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS**

- Les cas où les renseignements personnels sont nécessaires pour s'acquitter d'un mandat ou remplir un contrat de services réalisés par un tiers constituent aussi des exceptions. Cette exception a toutefois certaines conditions:
  - Le tiers doit posséder un mandat écrit qui détaille ses responsabilités à l'égard des renseignements personnels et les mesures de sécurité en place pour en assurer la protection.
  - Un accord écrit doit exiger du tiers qu'il avise le responsable de la protection des renseignements personnels de l'organisation chargé de recueillir les renseignements de toute violation ou tentative de violation de la confidentialité

### **8.3. Confidentialité technologique**

Les paramètres de confidentialité de toute technologie ou solution technologique utilisée par Locweld est réglés par défaut au **niveau le plus strict** en ce qui concerne les renseignements personnels.

### **8.4. Destruction des renseignements personnels**

Il est obligatoire de détruire un renseignement personnel lorsque les fins pour lesquelles il a été recueilli sont accomplies. S'il existe une raison légitime de conserver le renseignement, il est nécessaire de le rendre anonyme, à l'exception des dossiers des employés qui doivent être conserver selon le délai légal. Un délai peut être prolongé dans le cas d'un litige en cours.

### **8.5. Droit à l'oubli:**

Locweld doit accommoder les personnes qui souhaitent se prévaloir de leur droit de faire cesser la diffusion d'un renseignement personnel ou de désindexer ou réindexer un hyperlien rattaché à leur nom permettant d'accéder à ce renseignement.

*Le genre masculin est utilisé dans la présente politique comme genre neutre. L'emploi du genre masculin a pour but d'alléger le texte et d'en faciliter la lecture.*