

**POLITIQUE DE CYBERSÉCURITÉ
ET PROTECTION DES
RENSEIGNEMENTS PERSONNELS**

LA PATTE ADMINISTRATIVE INC.

RENSEIGNEMENTS PERSONNELS

Emilie Fracheboud, actionnaire et présidente de La Patte Administrative inc. est nommée officiellement responsable des renseignements personnels.

INVENTAIRE DES RENSEIGNEMENTS PERSONNELS

| INFORMATIONS | EMPLOYÉS | CLIENTS | VISITEURS | PROSPECTS |
|--------------------------|----------|---------|-----------|-----------|
| Nom | X | X | X | X |
| Adresse d'entreprise | | X | X | X |
| Adresse privée | X | X | | |
| NAS | X | X | | |
| Date de naissance | X | X | | |
| Téléphone privé | X | X | X | X |
| Téléphone entreprise | | X | X | X |
| Courriel | X | X | X | X |
| Site web | | X | X | X |
| Réseaux sociaux | X | X | X | X |
| NEQ/NE | | X | | |
| No de TPS/TVQ | | X | | |
| No employeur | | X | | |
| Spécimen de chèque | X | X | | |
| Accès bancaire | | X | | |
| Accès à divers logiciels | | X | | |

REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ

Un registre des incidents de confidentialité est tenu en cas d'atteinte à la confidentialité d'un renseignement personnel.

Un registre sur le modèle suivant est à remplir en cas d'incident et doit être communiqué à la Commission d'accès à l'information ainsi que la ou les personnes visées par l'incident

| Date de l'incident Ou découverte | Type d'incident | Renseignements visés par l'incident | Support de conservation des renseignements | Nombre de personnes visées par l'incident | Mesures prises dès la découverte de l'incident |
|----------------------------------|-----------------|-------------------------------------|--|---|--|
|----------------------------------|-----------------|-------------------------------------|--|---|--|

MESURES DE CYBERSÉCURITÉ

Plusieurs mesures sont mises en place afin de s'assurer une sécurité supérieure quant à la protection des données personnels et dans le cadre de la cybersécurité :

- Les mots de passes de l'entreprises et ceux conservés pour les clients sont enregistrés sur un logiciel externe à Zoho One
- Pour chaque client qui signe un contrat de service et par conséquent, pour qui on réalise un travail, nous tenons un registre des informations et mots de passe détenues pour ce client
- Une copie de sécurité de ces mots de passe est enregistrée sur le disque dur général de l'entreprise 1x par semaine.
- Une EDR est installé sur chacun des ordinateurs de l'entreprise. Une vérification quotidienne est faite de par le biais d'une agence de cybersécurité
- Chaque ordinateur de l'entreprise est connecté en continue à une application de VPN. Les employés de l'entreprise ont l'obligation de garder cette application allumée en tout temps. Si, dans le cas où un site nous refuse l'accès car on utilise un VPN (par exemple, site du gouvernement), une déconnexion temporaire de l'application est autorisée. Celle-ci doit être réactivée dès que l'utilisation du site en question est terminée
- Une sauvegarde des systèmes est effectuée une fois par mois. Les copies des sauvegardes est tenue sur un disque dur externe
- Tous les employés ont l'obligation de maintenir un pare-feu activé en tout temps
- Une vérification hebdomadaire par les employés du respect des mesures de cybersécurité est obligatoire
- Chaque employé de l'entreprise a suivi une formation de cybersécurité offerte par le FCEI
- Tous les employés de l'entreprise doivent uniquement conserver leurs mots de passe sur notre logiciel. Ils ont l'obligations de créer des mots de passe très sécurisés composés de majuscules, minuscules, lettres et chiffres et signes. Aucun mot de passe ne doit être utilisé 2x. Les employés doivent utiliser, si disponible l'authentications à deux facteurs.
- Notre site web est géré sur Wix et est sécurisé.
- Notre site de formation est géré par Thinkific et est sécurisé.
- Une bannière de demande d'autorisation de cookies est présente sur nos site web

- Tous les documents et disques durs externes de l'entreprise sont conservés dans une pièce sécurisée et fermée à clé.
- Les données de l'entreprise et des clients sont conservées sur le logiciel ZOHO One qui utilise un AES, l'une des plus robustes et puissantes méthodes de chiffrement des données sensibles

LISTE DE GESTION DES ACCÈS

| INFORMATIONS | CEO | Adjointe comptable et administrative | Adjointe marketing | Collaborations |
|---------------------------|-----|--------------------------------------|--------------------|----------------|
| Nom | X | X | X | X |
| Adresse d'entreprise | X | X | X | X |
| Adresse privée | X | X | X | |
| NAS | X | X | X | |
| Date de naissance | X | X | X | |
| Téléphone privé | X | X | X | X |
| Téléphone entreprise | X | X | X | X |
| Courriel | X | X | X | X |
| Site web | X | X | X | X |
| Réseaux sociaux | X | | X | |
| NEQ/NE | X | X | X | |
| No de TPS/TVQ | X | X | X | |
| No employeur | X | X | X | |
| Specimen de chèque | X | X | X | |
| Accès bancaire | X | X | | |
| Accès à divers logiciels | X | X | | |
| Informations des employés | X | X | X | |

POLITIQUES DE GOUVERNANCE DES RENSEIGNEMENTS PERSONNELS

Plusieurs mesures sont mises en place afin de s'assurer une sécurité supérieure quant à la protection des données.

Collecte de renseignements

- Une politique de confidentialité et de collecte de renseignement est publiée sur notre site pour encadrer l'utilisation des données provenant de l'utilisation du site web
- Une politique de confidentialité et de collecte de renseignement inscrite sur notre contrat de services afin d'encadrer les données collectées et utilisées dans le cadre de nos services.

Conservation et destruction des renseignements

Nous conservons les données reçues par les clients et utilisateurs du site web aussi longtemps que nous en avons besoin.

Dans le cadre de nos services, si nous n'effectuons pas de services pendant plus de 12 mois, nous restituons toutes les informations au client et supprimons ces données de nos systèmes

Rôles et responsabilités des membres de l'entreprise

Employés

Nous pouvons divulguer à tout membre de notre organisation les données utilisateur dont il a raisonnablement besoin pour réaliser les objectifs énoncés dans la présente politique.

Tierces parties

Nous pouvons partager les données utilisateur avec les tiers suivants :

- Collaborations mentionnées sur le site

Nous pouvons partager les données utilisateur avec des tiers aux fins suivantes :

- Répondre à votre demande de services

Les tiers ne seront pas en mesure d'accéder aux données des utilisateurs au-delà de ce qui est raisonnablement nécessaire pour atteindre l'objectif donné.

Autres divulgations

Nous nous engageons à ne pas vendre ou partager vos données avec des tiers, sauf dans les cas suivants :

- Si la loi l'exige
- Si elle est requise pour toute procédure judiciaire
- Pour prouver ou protéger nos droits légaux
- À des acheteurs ou des acheteurs potentiels de cette société dans le cas où nous cherchons à la vente de la société

Si vous suivez des hyperliens de notre site vers un autre site, veuillez noter que nous ne sommes pas responsables et n'avons pas de contrôle sur leurs politiques et pratiques de confidentialité.

Processus de traitement des plaintes relatives à la protection des renseignements

Si vous souhaitez que vos renseignements soient supprimés ou modifiés d'une façon ou d'une autre, veuillez communiquer avec notre agent de protection des renseignements confidentiels :

Emilie Fracheboud
emilie@lpadministrative.com
581 232-3029