JUMINE

Politique de protection des renseignements personnels

Version 3.3 | Adoptée le 4 août 2026 | Révision prévue en août 2028

La présente politique établit, en termes simples et clairs, les règles encadrant la protection des renseignements personnels détenus par Jumine inc. Elle est adoptée en application de la Loi sur la protection des renseignements personnels dans le secteur privé, modifiée par la Loi 25, et elle est proportionnée à la nature et à l'importance des activités de l'entreprise, qui est une petite entreprise.

Elle s'applique à toute personne agissant pour le compte de Jumine, soit les employés, les stagiaires, les consultants et les fournisseurs.

1. Responsable de la protection des renseignements personnels

Une personne désignée assume cette responsabilité. Elle approuve la présente politique, traite les demandes et les plaintes, détermine les suites à donner à tout incident et autorise au préalable les opérations visées à la section 8. Toute question relative à l'application de la politique lui est adressée.

> **À compléter**
>
> Sébastien de Blois, Directeur Général | sébastien.deblois@jumine.ca
>
> Lorsque la fonction n'est pas exercée par le dirigeant principal, la désignation est consignée par écrit, datée et signée, puis conservée avec la présente politique.

2. Renseignements personnels détenus

Personnes concernées	Renseignements et finalités
Employés et consultants	Coordonnées, numéro d'assurance sociale, salaire, coordonnées bancaires et évaluations. Gestion de la relation d'emploi, versement de la rémunération et respect des obligations fiscales et légales.
Candidats	Curriculum vitae, coordonnées et notes d'entrevue. Évaluation des candidatures.
Clients et contacts d'affaires	Nom, employeur, coordonnées professionnelles, données contractuelles et de facturation. Négociation et exécution des contrats, facturation et soutien.
Utilisateurs d'OptimaVue	Identifiant, nom, courriel professionnel, rôle et journaux de connexion. Gestion des comptes, sécurité des accès et soutien technique.
Visiteurs utilisant le formulaire de contact	Nom, courriel, entreprise et contenu du message. Réponse à la demande et suivi commercial.

Les données de procédé et les images captées dans les usines des clients ne permettent pas d'identifier une personne et ne constituent donc pas des renseignements personnels. Le site jumine.ca ne dépose aucun témoin de connexion et ne recueille aucun renseignement en dehors du formulaire de contact.

Le numéro d'assurance sociale est recueilli uniquement au moment de l'embauche et à des fins fiscales exclusivement. Il ne sert ni d'identifiant de dossier ni de preuve d'identité.

3. Règles applicables au personnel

- Ne recueillir que les renseignements nécessaires aux finalités déterminées. En cas de doute, s'abstenir.
- Informer la personne des finalités de la collecte ainsi que des moyens d'accéder à ses renseignements, de les faire rectifier ou de les faire supprimer. Le formulaire de contact du site affiche cette mention avant l'envoi et renvoie vers la présente politique.
- N'utiliser les renseignements qu'aux finalités annoncées lors de la collecte.
- N'accéder qu'aux renseignements nécessaires à l'exercice de ses fonctions.
- Ne communiquer aucun renseignement à l'extérieur de l'entreprise sans l'autorisation du responsable.
- Aviser le responsable dès qu'un doute ou une anomalie survient.

Le consentement peut être retiré en tout temps. L'utilisation d'un renseignement sensible, notamment de nature médicale, exige un consentement exprès. Une case cochée par défaut ne constitue pas un consentement valide.

4. Mesures de sécurité

- Authentification à deux facteurs sur tous les systèmes contenant des renseignements personnels.
- Chiffrement des ordinateurs portables et des sauvegardes.
- Accès accordés selon le besoin réel, revus annuellement et retirés le jour du départ d'une personne.
- Dossiers de paie conservés séparément, avec un nombre restreint de personnes autorisées.
- Aucun renseignement personnel réel dans les environnements de test.
- Engagement de confidentialité signé à l'embauche et séance de rappel annuelle destinée à l'ensemble du personnel.

5. Conservation et destruction

Les renseignements sont conservés pour la seule durée nécessaire à la réalisation des finalités, puis détruits de façon irréversible. Les documents papier sont déchiquetés et les supports numériques sont effacés de façon sécuritaire, sauvegardes comprises.

Renseignements	Durée	Point de départ
Paie, pièces fiscales et registre des employés	7 ans	Fin de l'année visée
Autres éléments du dossier d'employé	3 ans	Fin de l'emploi
Candidature non retenue	12 mois	Fin du processus de dotation
Dossiers clients, contrats et facturation	6 ans	Fin de l'exercice

Renseignements	Durée	Point de départ
Compte utilisateur OptimaVue	12 mois	Désactivation du compte
Message reçu par le formulaire de contact	12 mois	Dernier échange
Registre des incidents	5 ans	Prise de connaissance

Une conservation prolongée est permise lorsqu'un litige est en cours ou raisonnablement prévisible. Le motif est alors consigné par écrit.

6. Demandes et plaintes

Toute personne peut demander l'accès à ses renseignements, leur rectification, leur communication dans un format technologique structuré et couramment utilisé, ou la cessation de leur diffusion. Elle peut également porter plainte quant au respect de la présente politique.

1. La demande est adressée au responsable. Toute demande reçue par un autre membre du personnel lui est transmise le jour même.
2. Le responsable vérifie l'identité du demandeur et répond par écrit dans les 30 jours de la réception. L'absence de réponse équivaut à un refus.
3. Tout refus est motivé et informe la personne de son recours devant la Commission d'accès à l'information.
4. À la suite d'une rectification, le responsable en transmet une copie au demandeur et notifie la rectification aux tiers à qui le renseignement a été communiqué au cours des six mois précédents.

7. Incidents de confidentialité

Constituent notamment des incidents la perte ou le vol d'un appareil, l'envoi d'un courriel au mauvais destinataire, la compromission d'un mot de passe et une attaque par rançongiciel.

1. Aviser le responsable dans les 24 heures. Ne procéder à aucune suppression.
2. Contenir l'incident, soit révoquer les accès compromis, isoler les systèmes touchés et préserver les traces.
3. Le responsable évalue le risque de préjudice sérieux pour les personnes concernées et consigne sa conclusion par écrit, y compris lorsqu'elle est négative.
4. Lorsque le risque est établi, il avise la Commission d'accès à l'information avec diligence, puis les personnes concernées.
5. Il inscrit l'incident au registre, conservé cinq ans. Tous les incidents y sont inscrits, quelle que soit leur gravité.

> **Principe directeur**
>
> En cas de doute, l'événement est signalé. Sa qualification relève du responsable et non de la personne qui le constate. Aucun signalement fait de bonne foi n'entraîne de conséquence défavorable.

8. Opérations soumises à autorisation préalable

L'autorisation du responsable est requise avant de procéder à l'une des opérations suivantes.

- Acquérir, développer ou refondre un système d'information traitant des renseignements personnels.
- Héberger ou communiquer des renseignements personnels à l'extérieur du Québec. Une évaluation écrite doit alors démontrer que la protection y est adéquate et une entente écrite doit être conclue.
- Confier des renseignements personnels à un nouveau fournisseur. Le contrat écrit doit limiter l'usage au mandat, prévoir la destruction à l'échéance, imposer un avis sans délai en cas de violation et fixer le lieu d'hébergement.
- Ajouter une caméra ou en modifier la résolution lorsque cela pourrait rendre une personne identifiable, ou ajouter une fonction de localisation, de biométrie ou de profilage.
- Confier à un système automatisé une décision au sujet d'une personne sans possibilité de révision par un membre du personnel.

9. Documentation conservée

Le responsable tient un fichier unique regroupant quatre volets. Le registre des incidents, conservé cinq ans. Les demandes et les plaintes, avec les dates de réception et de réponse. La liste des systèmes utilisés et des pays d'hébergement. Les autorisations accordées en vertu de la section 8.

10. Diffusion, manquements et révision

La présente politique est publiée sur le site jumine.ca, accessible par un lien permanent placé au pied de chaque page. Elle est également remise à l'ensemble du personnel et transmise sans frais à toute personne qui en fait la demande au responsable. Toute modification est publiée avant son entrée en vigueur et la version en ligne porte sa date d'adoption.

La politique est révisée tous les deux ans, ou plus tôt en cas de modification législative ou de changement significatif aux activités de Jumine. Tout manquement peut entraîner des mesures disciplinaires pouvant aller jusqu'au congédiement, ou la résiliation du contrat d'un fournisseur. Pour l'entreprise, la Commission d'accès à l'information peut imposer des sanctions importantes, et la mise en œuvre documentée de la présente politique constitue un facteur atténuant reconnu.

> **Mise en ligne**
>
> Le lien doit pointer vers une adresse stable, par exemple jumine.ca/confidentialite, qui renvoie toujours vers la version en vigueur. Un lien contenant le numéro de version se brise à chaque révision.
>
> Le même lien est placé sous le formulaire de contact, ce qui répond à l'obligation d'informer la personne au moment de la collecte. Les coordonnées du responsable doivent être remplies avant la mise en ligne, puisque leur publication est elle-même une obligation légale.

Rôle	Nom et signature	Date
Responsable de la protection des renseignements personnels	Sébastien de Blois 	23 septembre 2026
Dirigeant principal	Sébastien de Blois	23 septembre 2026