

[NOM DE L'ENTREPRISE]

Politique d'utilisation de l'intelligence artificielle en entreprise

Modèle à intégrer au manuel de l'employé, conforme à la Loi 25

Section du manuel de l'employé : Politiques et procédures

Version : [1.0] · Date d'entrée en vigueur : [JJ mois AAAA] · Prochaine révision : [JJ mois AAAA]

Responsable de la protection des renseignements personnels : [NOM, TITRE, COURRIEL]

NOTE D'ADAPTATION (à retirer avant diffusion aux employés)

Ce modèle est conçu pour être adapté puis inséré tel quel dans un manuel de l'employé. Remplacez tous les champs entre crochets, par exemple [NOM DE L'ENTREPRISE], par les informations propres à votre organisation.

Faites valider la version finale par un conseiller juridique ou par votre responsable de la protection des renseignements personnels (RPRP) avant diffusion, particulièrement les sections 5, 6 et 9 qui dépendent des licences d'outils réellement utilisées dans votre entreprise.

Les règles ci-dessous se veulent un minimum raisonnable pour une PME québécoise. Ajustez-les à la taille, au secteur d'activité et aux outils réellement déployés chez vous.

Table des matières

Clic droit sur la table ci-dessus dans Word, puis « Mettre à jour les champs », pour générer automatiquement les numéros de page.

1. Objet et champ d'application

La présente politique encadre l'utilisation des outils d'intelligence artificielle générative, dont ChatGPT, Microsoft Copilot et Google Gemini, par l'ensemble du personnel de [NOM DE L'ENTREPRISE], que ce soit sur des appareils fournis par l'entreprise ou des appareils personnels utilisés dans le cadre du travail.

Elle s'applique à toute personne salariée, stagiaire, personne contractante ou consultante qui a accès aux systèmes, aux documents ou aux renseignements personnels de [NOM DE L'ENTREPRISE], sans égard à son statut d'emploi ou à son lieu de travail.

Cette politique répond aux obligations de gouvernance des renseignements personnels imposées par la Loi 25, soit la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*¹, qui exige que toute entreprise exploitée au Québec, peu importe sa taille, adopte des politiques encadrant la gouvernance des renseignements personnels tout au long de leur cycle de vie.²

2. Cadre légal de référence

La présente politique s'appuie notamment sur :

- La *Loi sur la protection des renseignements personnels dans le secteur privé* (RLRQ c. P-39.1), telle que modifiée par la Loi 25;³
- Les orientations et outils publiés par la Commission d'accès à l'information du Québec (CAI);
- Le *Code civil du Québec* (articles 35 à 40) sur le respect de la vie privée;
- Les conditions d'utilisation et les engagements contractuels de confidentialité des fournisseurs d'outils d'IA retenus par [NOM DE L'ENTREPRISE].

Le non-respect de la Loi 25 expose [NOM DE L'ENTREPRISE] à des sanctions administratives pouvant atteindre 10 millions de dollars ou 2 % du chiffre d'affaires mondial, ainsi qu'à des sanctions pénales pouvant atteindre 25 millions de dollars ou 4 % du chiffre d'affaires mondial, selon le montant le plus élevé.⁴ Le respect de cette politique par chaque employé est donc essentiel à la protection de l'entreprise et de sa clientèle.

¹Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (Loi 25), RLRQ c. P-39.1. legisquebec.gouv.qc.ca/fr/document/lc/p-39.1

²Commission d'accès à l'information du Québec, « Principaux changements apportés par la Loi 25 ». cai.gouv.qc.ca/protection-renseignements-personnels/sujets-et-domaines-dinteret/principaux-changements-loi-25

³Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (Loi 25), RLRQ c. P-39.1. legisquebec.gouv.qc.ca/fr/document/lc/p-39.1

⁴Gouvernement du Québec, « Loi 25 sur la protection des renseignements personnels des citoyens du Québec », sanctions administratives pouvant atteindre 10 M\$ ou 2 % du chiffre d'affaires mondial, et sanctions pénales jusqu'à 25 M\$ ou 4 %. quebec.ca/nouvelles/actualites

3. Définitions

Intelligence artificielle générative : outil capable de produire du texte, des images, du code ou d'autres contenus à partir d'instructions fournies par une personne utilisatrice, par exemple ChatGPT, Microsoft Copilot ou Google Gemini.

Renseignement personnel : toute information qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier (nom, courriel, numéro de téléphone, adresse IP, numéro d'assurance sociale, dossier médical, dossier RH, historique d'achats, etc.).

Outil grand public : version gratuite ou personnelle d'un outil d'IA (par exemple ChatGPT Free ou Plus, Copilot avec compte Microsoft personnel, Gemini avec compte Gmail personnel), non couverte par une entente contractuelle avec [NOM DE L'ENTREPRISE].

Hallucination : réponse produite par un outil d'IA qui semble crédible mais qui est fausse, inventée, inexacte ou non vérifiable dans une source fiable.

Incident de confidentialité : accès, utilisation, communication, perte de renseignements personnels non autorisés par la loi, ou atteinte à leur protection, notamment par la saisie de tels renseignements dans un outil d'IA non autorisé.

RPRP : Responsable de la protection des renseignements personnels, désigné conformément à la Loi 25. À défaut d'une autre désignation, cette fonction est exercée par la personne ayant la plus haute autorité au sein de [NOM DE L'ENTREPRISE].⁵

4. Principes généraux d'utilisation

- L'IA est un outil d'appui au travail, jamais un substitut au jugement professionnel. Toute production issue de l'IA doit être relue et validée par une personne avant d'être utilisée ou transmise.
- Seuls les comptes professionnels autorisés par [NOM DE L'ENTREPRISE] (section 5) peuvent être utilisés pour des tâches liées au travail.
- Aucun renseignement personnel ni aucun document confidentiel ne doit être saisi dans un outil d'IA grand public (section 6).
- Chaque personne employée demeure responsable du contenu qu'elle produit ou transmet, même lorsqu'il a été généré ou assisté par une IA.
- Toute erreur, tout doute ou toute hallucination détectée doit être signalé sans délai selon la procédure décrite à la section 8.
- En cas de doute sur un usage précis, la personne employée doit s'abstenir et consulter [RESPONSABLE TI OU RPRP] avant d'agir.

⁵Commission d'accès à l'information du Québec, « Principaux changements apportés par la Loi 25 ». cai.gouv.qc.ca/protection-renseignements-personnels/sujets-et-domaines-dinteret/principaux-changements-loi-25

5. Règles d'utilisation de ChatGPT, Copilot et Gemini

Le tableau ci-dessous résume les usages autorisés et interdits pour les principaux outils d'IA utilisés chez [NOM DE L'ENTREPRISE]. La règle centrale : seule une version professionnelle, liée au compte de l'entreprise et couverte par une entente excluant l'utilisation des données à des fins d'entraînement des modèles, peut servir pour des tâches de travail.

Outil	Usages autorisés	Usages interdits
ChatGPT (OpenAI)	- Compte professionnel [NOM DE L'ENTREPRISE] de type ChatGPT Team ou Enterprise, avec entraînement des modèles désactivé par contrat - Rédaction, résumé, brainstorm, traduction de contenus non confidentiels - Aide à la programmation sur du code ne contenant aucune donnée client	- Compte grand public (Free, Plus, Pro) payé personnellement par l'employé pour des tâches de travail - Téléversement de documents contenant des renseignements personnels ou confidentiels - Utilisation de réponses sans vérification pour des communications officielles ou des décisions RH
Microsoft Copilot	- Copilot Chat ou Microsoft 365 Copilot lié au compte professionnel Microsoft de [NOM DE L'ENTREPRISE] (protection des données d'entreprise activée) - Analyse de documents internes déjà hébergés dans l'environnement Microsoft 365 de l'entreprise	- Connexion avec un compte Microsoft personnel - Bascule vers le mode « Web » pour traiter des documents confidentiels - Partage de renseignements personnels de clients ou d'employés en dehors des outils autorisés
Google Gemini	- Gemini pour Google Workspace lié au compte professionnel de [NOM DE L'ENTREPRISE] - Assistance à la rédaction dans Docs, Sheets ou Gmail professionnels	- Compte Gemini personnel (@gmail.com) - Téléversement de contrats, dossiers clients ou dossiers d'employés
Tout autre outil d'IA (Claude, Perplexity, DeepSeek, outils non listés, etc.)	- Usage soumis à autorisation préalable du [RESPONSABLE TI OU RPRP] - Recherche d'information publique, veille, idéation générale	Tout usage non approuvé impliquant des documents ou des données de l'entreprise

5.1 Pourquoi cette distinction

Les comptes grand public (gratuits ou personnels) de ChatGPT, Copilot et Gemini peuvent conserver et utiliser les conversations pour améliorer leurs modèles, sauf désactivation manuelle par la personne

utilisatrice. Les versions professionnelles sous licence (ChatGPT Team ou Enterprise, Microsoft 365 Copilot, Gemini pour Google Workspace) sont couvertes par des ententes contractuelles excluant cet usage et, dans le cas de Microsoft 365 Copilot, respectent les permissions déjà en vigueur dans l'environnement de l'entreprise.⁶

5.2 Accès et autorisation

- L'accès aux outils d'IA professionnels est accordé par [RESPONSABLE TI] selon les besoins du poste.
- L'utilisation d'un outil d'IA non listé dans le tableau ci-dessus doit être approuvée au préalable par [RESPONSABLE TI OU RPRP].
- Il est interdit d'installer des extensions, greffons ou applications tierces reliées à un outil d'IA sans autorisation.

6. Interdiction de saisir des renseignements personnels dans les outils grand public

Il est strictement interdit de saisir, coller, téléverser ou dicter un renseignement personnel, qu'il s'agisse d'un client, d'un employé, d'un fournisseur ou de toute autre personne, dans un outil d'IA grand public. Cette règle découle directement des obligations de gouvernance imposées par la Loi 25.⁷

6.1 Exemples de renseignements visés

- Nom complet combiné à une adresse, un numéro de téléphone ou un courriel personnel;
- Numéro d'assurance sociale, numéro de permis de conduire, numéro d'assurance maladie;
- Dossier RH (évaluation, salaire, mesure disciplinaire, absence pour maladie);
- Dossier client ou dossier de crédit, numéro de carte de paiement;
- Toute donnée de santé, situation financière ou donnée biométrique;
- Photos ou enregistrements permettant d'identifier une personne.

6.2 Ce qu'il faut faire à la place

- Retirer ou remplacer les renseignements personnels par des exemples génériques ([NOM DU CLIENT], [MONTANT]) avant d'utiliser un outil d'IA grand public;
- Utiliser uniquement l'outil professionnel homologué (section 5) lorsque le traitement de renseignements personnels est nécessaire;
- Consulter [RESPONSABLE TI OU RPRP] si une tâche semble exiger l'usage de renseignements personnels dans un outil d'IA.

⁶Microsoft Learn, « Protection des données d'entreprise dans Microsoft 365 Copilot et Microsoft 365 Copilot Chat ». learn.microsoft.com/fr-fr/microsoft-365/copilot/enterprise-data-protection

⁷Commission d'accès à l'information du Québec, « Principaux changements apportés par la Loi 25 ». cai.gouv.qc.ca/protection-renseignements-personnels/sujets-et-domaines-dinteret/principaux-changements-loi-25

6.3 Cas particulier des mineurs

Conformément à la Loi 25, la collecte, l'utilisation ou la communication de renseignements personnels concernant une personne de moins de 14 ans requiert le consentement du titulaire de l'autorité parentale ou du tuteur. Aucun renseignement concernant un mineur ne doit être saisi dans un outil d'IA, quel qu'il soit, sans validation préalable du [RPRP].

7. Partage de documents confidentiels avec des services infonuagiques

Avant de téléverser, coller ou partager un document dans un outil d'IA ou tout autre service infonuagique, chaque personne employée doit d'abord identifier le niveau de confidentialité du document, selon le tableau suivant.

Catégorie	Exemples	Règle avec les outils d'IA grand public
Public	Contenu du site web, communiqués, publications marketing déjà publiées	Utilisation libre
Interne	Procédures internes génériques, modèles de courriels sans nom de client	Permise avec un compte professionnel autorisé (section 5)
Confidentiel	Contrats, listes de clients, données financières, dossiers RH, plans stratégiques	Interdite dans tout outil grand public. Autorisée uniquement dans l'outil d'entreprise homologué par [RESPONSABLE TI]
Hautement confidentiel ou protégé	Renseignements personnels sensibles (santé, situation financière, numéros d'assurance sociale, données biométriques), secrets commerciaux	Interdite dans tout outil d'IA, même professionnel, sauf autorisation écrite préalable du [RPRP]

7.1 Liste de vérification avant tout téléversement

1. Ce document contient-il des renseignements personnels ou des données de nature confidentielle? Si oui, arrêter et consulter la section 6.
2. L'outil utilisé est-il un compte professionnel autorisé par [NOM DE L'ENTREPRISE] (section 5)? Sinon, ne pas procéder.
3. Les paramètres de confidentialité du compte empêchent-ils l'utilisation des données à des fins d'entraînement des modèles? Vérifier auprès de [RESPONSABLE TI] en cas de doute.
4. Le document est-il nécessaire dans son intégralité, ou une version cachée ou résumée des passages sensibles suffit-elle?
5. Le partage a-t-il été autorisé par la personne responsable du dossier ou par [RPRP], le cas échéant?

7.2 Consignes générales

- Ne jamais téléverser de contrats, dossiers clients, dossiers RH, données financières ou documents stratégiques dans un outil d'IA grand public ou un service infonuagique non approuvé;

- Privilégier les outils d'entreprise dont les serveurs et les conditions de traitement des données ont été validés par [RESPONSABLE TI];
- Ne jamais utiliser un outil d'IA pour contourner un mot de passe, un chiffrement ou une protection appliquée à un document;
- Supprimer les copies temporaires ou les historiques de conversation contenant des documents confidentiels dès que la tâche est terminée, lorsque l'outil le permet;
- Signaler immédiatement tout téléversement accidentel d'un document confidentiel dans un outil non autorisé, selon la procédure de la section 9.

8. Signalement des erreurs et des hallucinations de l'IA

Les outils d'IA générative peuvent produire des réponses inexactes, incomplètes ou complètement inventées, même lorsqu'elles semblent crédibles. Chaque personne employée a la responsabilité de vérifier les résultats produits par l'IA avant de les utiliser, et de signaler toute erreur significative.

8.1 Quand signaler

- Une réponse contient une information fausse, une statistique inventée ou une source qui n'existe pas;
- Une réponse a été utilisée par erreur dans un document destiné à un client, à un partenaire ou au public avant d'être corrigée;
- Un outil d'IA a produit un contenu discriminatoire, biaisé ou inapproprié;
- Un renseignement personnel ou confidentiel a été saisi par erreur dans un outil non autorisé (voir aussi section 9).

8.2 Marche à suivre

6. Cesser d'utiliser ou de diffuser le contenu concerné dès que l'erreur est constatée.
7. Si le contenu a déjà été transmis à une personne externe, en informer immédiatement [RESPONSABLE / SUPERVISEUR IMMÉDIAT].
8. Remplir le formulaire de signalement (annexe B) en décrivant l'outil utilisé, la question posée, la réponse reçue et l'erreur constatée.
9. Transmettre le formulaire à [RESPONSABLE TI OU RPRP / ADRESSE COURRIEL DÉDIÉE].
10. Conserver une copie de la conversation en cause, dans la mesure du possible, pour appuyer l'analyse.

Les signalements sont consignés dans un registre interne afin de repérer les outils ou les usages qui génèrent des erreurs récurrentes et d'ajuster la formation ou les outils autorisés en conséquence.

9. Incidents de confidentialité liés à l'IA

La saisie non autorisée d'un renseignement personnel dans un outil d'IA grand public constitue un incident de confidentialité au sens de la Loi 25. Tout incident, même mineur ou sans conséquence apparente, doit être signalé sans délai.⁸

9.1 Marche à suivre immédiate

11. Ne pas tenter de « corriger » la situation seul : aviser immédiatement [RPRP / RESPONSABLE TI].
12. Si possible, retirer ou supprimer le renseignement personnel de la conversation ou du compte concerné.
13. Décrire par écrit ce qui a été saisi, dans quel outil, à quelle date et par qui.
14. Le [RPRP] évalue le risque de préjudice sérieux pour les personnes concernées et détermine si une déclaration à la Commission d'accès à l'information (CAI) et un avis aux personnes concernées sont requis.
15. Tout incident est consigné dans le registre des incidents de confidentialité de [NOM DE L'ENTREPRISE], même lorsqu'aucune déclaration externe n'est nécessaire.

Cette procédure reprend les obligations prévues par la Loi 25 : prendre les mesures raisonnables pour réduire les risques, aviser la CAI et les personnes concernées en cas de risque de préjudice sérieux, et tenir un registre de tous les incidents.⁹

10. Rôles et responsabilités

Direction : approuve la présente politique, alloue les ressources nécessaires à son application et désigne le RPRP.

Responsable de la protection des renseignements personnels (RPRP) : reçoit les signalements d'incidents, tient le registre des incidents, évalue le risque de préjudice sérieux et représente [NOM DE L'ENTREPRISE] auprès de la CAI au besoin. Ses coordonnées sont publiées et accessibles à tout le personnel.

Responsable TI : gère les accès aux outils d'IA professionnels, valide les paramètres de confidentialité et maintient la liste des outils autorisés.

Gestionnaires : s'assurent que leur équipe connaît et applique la présente politique et signalent tout usage préoccupant.

Personnel : applique la politique au quotidien, vérifie les résultats produits par l'IA et signale toute erreur ou tout incident sans délai.

⁸Fédération canadienne de l'entreprise indépendante (FCEI), « Tout ce que vous devez savoir sur la Loi 25 », obligations en cas d'incident de confidentialité. cfib-fcei.ca/fr/site/qc-loi-25

⁹Fédération canadienne de l'entreprise indépendante (FCEI), « Tout ce que vous devez savoir sur la Loi 25 », obligations en cas d'incident de confidentialité. cfib-fcei.ca/fr/site/qc-loi-25

11. Formation et sensibilisation

- Toute personne nouvellement embauchée reçoit une présentation de la présente politique dès son intégration.
- Une formation de rappel est offerte à l'ensemble du personnel au moins une fois par année, ou lors de l'ajout d'un nouvel outil d'IA.
- Les gestionnaires reçoivent une formation complémentaire sur la reconnaissance des incidents de confidentialité et la procédure de signalement.

12. Non-respect de la politique

Le non-respect de la présente politique peut entraîner des mesures disciplinaires pouvant aller jusqu'au congédiement, selon la gravité du manquement, en conformité avec les politiques RH de [NOM DE L'ENTREPRISE] et les dispositions légales applicables. Un manquement ayant entraîné un incident de confidentialité grave peut également exposer [NOM DE L'ENTREPRISE] à des sanctions réglementaires en vertu de la Loi 25.

13. Révision et mise à jour de la politique

La présente politique est révisée au moins une fois par année, ou plus fréquemment si de nouveaux outils d'IA sont déployés, si la réglementation évolue ou si un incident majeur en révèle la nécessité. Toute modification est communiquée à l'ensemble du personnel.

14. Entrée en vigueur et acceptation

La présente politique entre en vigueur le [JJ mois AAAA]. En signant ci-dessous, la personne employée reconnaît avoir pris connaissance de la politique, l'avoir comprise et s'engage à la respecter.

Nom de la personne employée : _____

Signature : _____ Date : _____

Annexe A. Tableau récapitulatif des outils autorisés

Outil	Usages autorisés	Usages interdits
ChatGPT (OpenAI)	• Compte professionnel [NOM DE L'ENTREPRISE] de type ChatGPT Team ou Enterprise, avec entraînement des modèles désactivé par contrat • Rédaction, résumé, brainstorm, traduction de contenus non confidentiels • Aide à la programmation sur du code ne contenant aucune donnée client	• Compte grand public (Free, Plus, Pro) payé personnellement par l'employé pour des tâches de travail • Téléversement de documents contenant des renseignements personnels ou confidentiels • Utilisation de réponses sans vérification pour des communications officielles ou des décisions RH
Microsoft Copilot	• Copilot Chat ou Microsoft 365 Copilot lié au compte professionnel Microsoft de [NOM DE L'ENTREPRISE] (protection des données d'entreprise activée) • Analyse de documents internes déjà hébergés dans l'environnement Microsoft 365 de l'entreprise	• Connexion avec un compte Microsoft personnel • Bascule vers le mode « Web » pour traiter des documents confidentiels • Partage de renseignements personnels de clients ou d'employés en dehors des outils autorisés
Google Gemini	• Gemini pour Google Workspace lié au compte professionnel de [NOM DE L'ENTREPRISE] • Assistance à la rédaction dans Docs, Sheets ou Gmail professionnels	• Compte Gemini personnel (@gmail.com) • Téléversement de contrats, dossiers clients ou dossiers d'employés
Tout autre outil d'IA (Claude, Perplexity, DeepSeek, outils non listés, etc.)	• Usage soumis à autorisation préalable du [RESPONSABLE TI OU RPRP] • Recherche d'information publique, veille, idée générale	• Tout usage non approuvé impliquant des documents ou des données de l'entreprise

Annexe B. Formulaire de signalement (erreur, hallucination ou incident)

À remplir par la personne employée et à transmettre à [RESPONSABLE TI OU RPRP / ADRESSE COURRIEL DÉDIÉE].

- Date et heure de l'événement : _____
- Nom de la personne qui signale : _____
- Outil d'IA utilisé (ChatGPT, Copilot, Gemini, autre) : _____
- Type d'événement : ☐ Erreur ou hallucination ☐ Renseignement personnel saisi par erreur ☐ Document confidentiel partagé ☐ Autre
- Description de la question posée à l'IA : _____
- Description de la réponse ou du contenu problématique : _____
- Le contenu a-t-il été diffusé ou transmis à une personne externe? ☐ Oui ☐ Non
- Mesures déjà prises par la personne qui signale : _____
- Section réservée au RPRP : évaluation du risque, mesures correctives, suivi requis auprès de la CAI (oui ou non) : _____

Annexe C. Aide-mémoire (à afficher ou à distribuer)

Les 5 règles à retenir :

16. J'utilise uniquement le compte professionnel autorisé, jamais un compte personnel, pour le travail.
17. Je ne saisis jamais de nom, courriel, numéro ou dossier de client ou d'employé dans un outil grand public.
18. Je vérifie toujours les réponses de l'IA avant de les utiliser ou de les transmettre.
19. Je signale immédiatement toute erreur, hallucination ou saisie accidentelle de renseignements personnels.
20. En cas de doute, je m'abstiens et je demande conseil à [RESPONSABLE TI OU RPRP].

Annexe D. Références

- [Loi sur la protection des renseignements personnels dans le secteur privé \(Loi 25\), LegisQuébec](#)
- [Commission d'accès à l'information, Principaux changements apportés par la Loi 25](#)
- [Gouvernement du Québec, Entrée en vigueur des dispositions de la Loi 25](#)
- [FCEI, Tout ce que vous devez savoir sur la Loi 25](#)
- [Microsoft Learn, Protection des données d'entreprise dans Microsoft 365 Copilot](#)