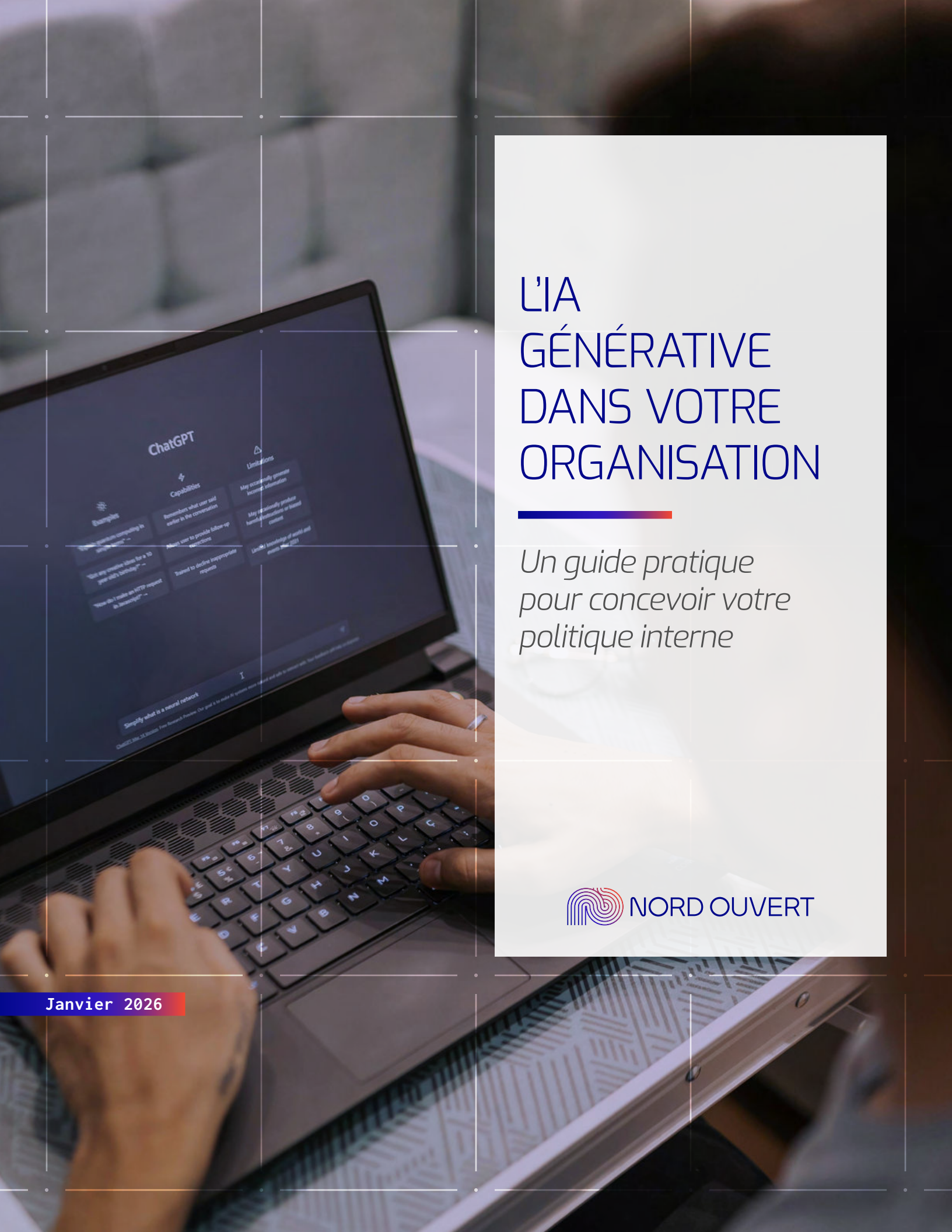


L'IA GÉNÉRATIVE DANS VOTRE ORGANISATION

Un guide pratique pour concevoir votre politique interne

NORD OUVERT

Janvier 2026

À PROPOS DE CE GUIDE

Ce guide est destiné aux petites et moyennes entreprises du Québec et du Canada. Il contient à la fois du contenu éducatif pour vous aider à comprendre les risques et les opportunités liés à l'intelligence artificielle (IA) générative, ainsi que des règles pratiques et concrètes que vous pouvez adapter à votre organisation.

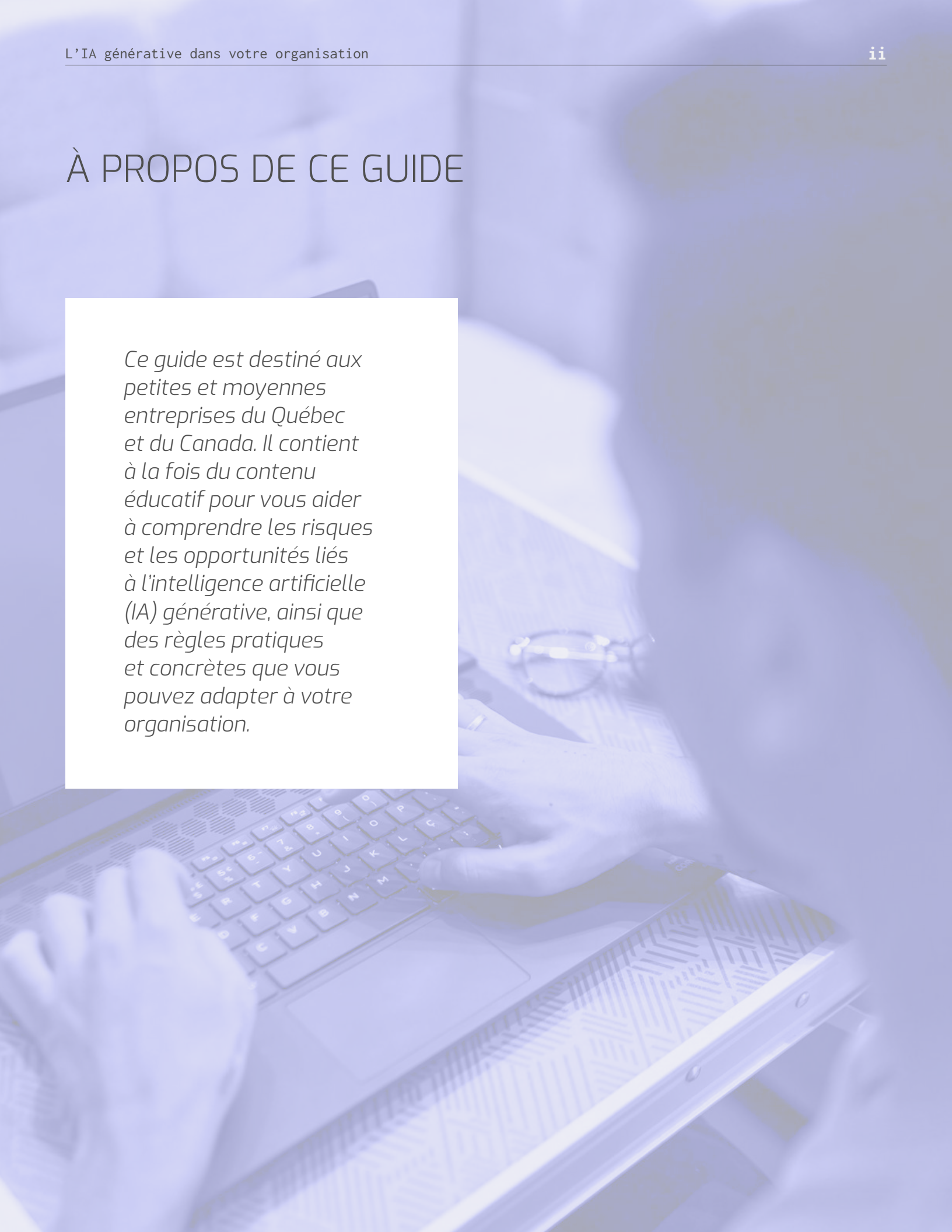


TABLE DES MATIÈRES

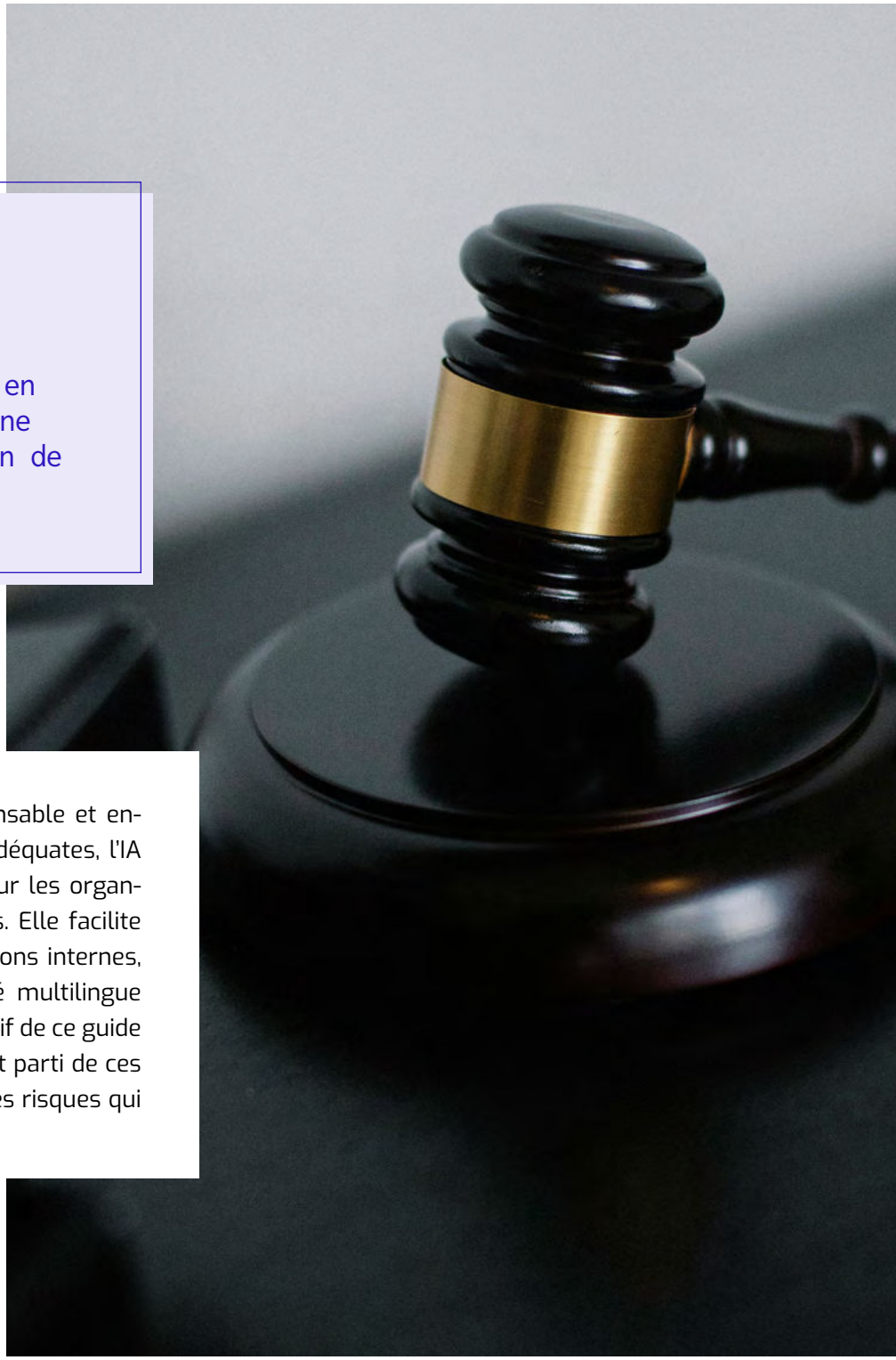
POURQUOI VOTRE ORGANISATION A BESOIN D'UNE POLITIQUE INTERNE EN MATIÈRE D'IA GÉNÉRATIVE

La réalité : l'IA est déjà présente sur votre lieu de travail

Les outils d'IA générative tels que ChatGPT, Microsoft Copilot et Google Gemini font désormais partie intégrante du quotidien professionnel. Certaines sources indiquent qu'environ 75 % des employés de bureau utilisent leurs propres outils d'IA au travail, et que plus de 60 % d'entre eux ignorent les politiques de leur entreprise en la matière. Cela donne naissance à ce que l'on appelle l'« IA fantôme » (en anglais, *Shadow AI*) : une utilisation non contrôlée qui expose votre entreprise à des risques invisibles et incontrôlables.

Risques documentés : cas réels, conséquences réelles

- **Responsabilité organisationnelle (Air Canada, 2024):** Dans l'affaire Moffatt c. Air Canada, le Tribunal de résolution des litiges civils de la Colombie-Britannique a jugé qu' Air Canada était responsable des informations erronées fournies par son agent conversationnel (*chatbot* en anglais). Le tribunal a rejeté l'argument selon lequel l'agent conversationnel était « une entité juridique distincte responsable de ses propres actions », affirmant qu'il devrait être « évident pour Air Canada qu'elle est responsable de toutes les informations figurant sur son site web ». Cette affaire établit que les organisations ne peuvent pas décliner leur responsabilité quant aux résultats de l'IA.
- **Exposition des données (Samsung, 2023) :** Dans les 20 jours suivant l'autorisation d'accès à ChatGPT, Samsung a subi trois fuites de données distinctes : du code source, du code d'optimisation de programme et des transcriptions de réunions. Une fois saisies, ces données deviennent irrécupérables sur les serveurs du fournisseur d'IA.
- **Hallucinations juridiques :** Les tribunaux au Canada et ailleurs dans le monde ont recensé des centaines de cas où des avocats ont présenté des citations juridiques fabriquées par l'IA. Dans l'affaire Zhang c. Chen (2024), un avocat de la Colombie-Britannique a été condamné à payer des frais pour avoir soumis de fausses références générées par l'IA. De même, dans l'affaire Reddy c. Saroya (2025), la Cour d'appel de l'Alberta a statué que les avocats assument la « responsabilité ultime » des erreurs de l'IA.
- **Biais et discrimination :** dans le cadre du règlement iTutorGroup EEOC (États-Unis, 2023), un outil de recrutement basé sur l'IA a automatiquement rejeté les candidatures de femmes de plus de 55 ans et d'hommes de plus de 60 ans. Cette pratique discriminatoire a entraîné le versement d'une indemnité de 365 000 $.



Point clé à retenir

Votre organisation est responsable de tous les résultats de l'IA utilisés en son nom. « L'IA a commis une erreur » n'est pas un moyen de défense juridique.

Saisir l'opportunité d'une IA responsable

Lorsqu'elle est déployée de façon responsable et encadrée par des mesures de protection adéquates, l'IA générative devient un véritable levier pour les organisations disposant de ressources limitées. Elle facilite notamment la rédaction de communications internes, la synthèse de documents, l'accessibilité multilingue ainsi que l'idéation et la recherche. L'objectif de ce guide est de vous permettre de tirer pleinement parti de ces avantages, tout en gérant efficacement les risques qui y sont associés..

QU'EST-CE QUE L'IA GÉNÉRATIVE? CONCEPTS CLÉS

Pour bien encadrer l'utilisation d'un outil, il faut d'abord en comprendre les rouages. Cette section propose des définitions essentielles, conçues pour offrir au personnel les connaissances nécessaires à une utilisation sécuritaire et éclairée de ces technologies.

Définitions essentielles

TERME	DÉFINITION (CE QUE VOUS DEVEZ SAVOIR)
Intelligence artificielle (AI) générative	Systèmes d'IA capables de créer de nouveaux contenus (textes, images, codes, fichiers audio) en s'appuyant sur des modèles appris à partir de données d'entraînement. Exemples : ChatGPT, Copilot, Gemini, Claude.
Hallucination	Phénomène par lequel l'IA génère un contenu qui semble plausible, mais qui est factuellement erroné ou inventé. Il s'agit d'une caractéristique fondamentale du fonctionnement de ces systèmes et non d'un bogue qui sera corrigé. Vérifiez toujours les résultats de l'IA et exigez des sources.
Invite (ou *prompt*)	Instruction ou commande saisie dans un système d'IA. Ne transmettez jamais de renseignements personnels, de données confidentielles ou de secrets commerciaux dans les invites d'outils d'IA publics.
Renseignements personnels	Toute information permettant d'identifier une personne : nom, coordonnées, identifiants, données de santé, dossiers financiers ou toute autre donnée qui, seule ou combinée à d'autres, permettrait d'identifier une personne.
IA fantôme (*Shadow AI*)	Utilisation non autorisée d'outils d'IA par le personnel, souvent par le biais de comptes personnels ou d'outils non approuvés. Cela crée des risques de conformité, de sécurité et de qualité que votre organisation ne peut ni voir ni gérer.

Types d'outils IA et profils de risque

TYPE D'OUTIL	EXEMPLES	RISQUES PRINCIPAUX
Outil infonuagique public (versions gratuites)	ChatGPT Free, Claude Free, Gemini Free, Perplexity Free, Copilot Free	**RISQUE ÉLEVÉ :** Les données peuvent être utilisées pour l'entraînement des modèles; les contrôles de confidentialité sont limités; les serveurs sont probablement situés hors du Canada. Veillez à ne jamais utiliser de renseignements confidentiels ou personnels.
Outil infonuagique public (versions payantes)	ChatGPT Plus ou Pro, Claude Pro ou Max, Gemini Pro ou Ultra, Perplexity Pro ou Max, Copilot Pro	**RISQUE MOYEN À ÉLEVÉ :** Une option de retrait (opt-out) à l'entraînement des modèles est généralement proposée; certains contrôles de confidentialité sont présents; les serveurs sont toujours susceptibles d'être hors du Canada. Veillez à ne jamais utiliser de renseignements confidentiels ou personnels. Vérifiez les politiques d'entraînement des données avant d'y soumettre des informations internes importantes.
Outil infonuagique d'entreprise	ChatGPT Enterprise, Microsoft 365 Copilot, Google Workspace AI	**RISQUE MOYEN :** Les données ne sont généralement pas utilisées pour l'entraînement des modèles; les contrôles de confidentialité sont supérieurs; l'utilisation de renseignements personnels dans ces outils nécessite au préalable une EFVP (Évaluation des facteurs relatifs à la vie privée). Assurez-vous de vérifier la localisation des serveurs de données et les conditions d'utilisation.
IA intégrée	IA dans Adobe, Canva, Zoom, extensions de navigateur	**RISQUE VARIABLE :** Souvent activée par défaut; examinez les conditions du fournisseur avant l'utilisation. Attention : les extensions d'IA pour navigateurs peuvent lire l'intégralité du contenu de vos pages Web.
Auto-hébergé	Llama, Mistral, autres modèles d'IA open source sur votre propre infrastructure	**RISQUE FAIBLE :** contrôle total des données; aucun partage externe. Nécessite une expertise technique.

Ce que l'IA générative ne peut pas faire

- **Garantir l'exactitude :** l'IA prédit un texte plausible, pas un texte correct. Elle peut affirmer avec certitude des informations fausses.
- **Garantir la confidentialité sur les outils publics :** les données saisies peuvent être stockées, consultées ou utilisées à des fins d'entraînement des modèles.
- **Remplacer le jugement humain :** pour les décisions qui touchent des personnes, l'examen humain est essentiel et souvent requis par la loi.

LE CADRE JURIDIQUE AU QUÉBEC, AU CANADA ET AU-DELÀ

Avertissement juridique

Cette section fournit des informations générales sur les exigences légales applicables. Elle ne constitue pas un avis juridique et doit être validée par vos conseillers juridiques et en matière de conformité. Les lois et règlements peuvent avoir changé depuis la publication de ce guide.

La Loi 25 du Québec désormais pleinement en vigueur

La Loi 25 est entrée pleinement en vigueur le 22 septembre 2024. Il s'agit actuellement de la loi la plus stricte en matière de protection de la vie privée au Canada. Si votre organisation exerce ses activités au Québec ou traite des données de résidents du Québec, vous devez vous y conformer. Voici les principales dispositions touchant l'utilisation de l'IA :

- **Décisions fondées sur un traitement automatisé (article 12.1) :** Lorsque les décisions sont prises exclusivement par le traitement automatisé de renseignements personnels, vous devez informer la personne concernée, lui expliquer les renseignements personnels utilisés, les raisons et les principaux facteurs qui ont conduit à la décision, et lui donner le droit de soumettre ses observations à une personne qui pourra réexaminer la décision.
- **Évaluations des facteurs relatifs à la vie privée (EFVP) :** Elles sont obligatoires avant d'acquérir ou de développer toute nouvelle technologie impliquant le traitement de renseignements personnels, ainsi qu'avant de communiquer de tels renseignements à l'extérieur du Québec. Notez que la plupart des outils infonuagiques d'IA sont considérés comme un transfert de données hors Québec.
- **Responsable désigné de la protection des renseignements personnels :** Par défaut, la personne la plus haut placée dans l'organisation est responsable de la conformité en matière de protection de la vie privée. Cette responsabilité peut être déléguée par écrit.
- **Données biométriques :** L'utilisation de systèmes d'identification biométrique doit être notifiée à la Commission d'accès à l'information (CAI) au moins 60 jours avant leur mise en œuvre.
- **Portabilité des données :** Les personnes ont le droit de demander leurs renseignements personnels dans un format structuré et couramment utilisé.

Sanctions : Les organisations s'exposent à des sanctions administratives pécuniaires pouvant atteindre 10 millions de dollars ou 2 % du chiffre d'affaires mondial de l'exercice précédent. En cas de poursuites pénales, ces amendes peuvent grimper jusqu'à 25 millions de dollars ou 4 % du chiffre d'affaires mondial. De plus, la loi prévoit un droit d'action privé permettant aux individus d'engager des poursuites civiles pour obtenir des dommages-intérêts, avec un montant minimal de 1 000 $ par personne en cas d'atteinte intentionnelle ou de faute lourde.

Directives importantes de la CAI

La Commission d'accès à l'information a publié des directives qui ont une incidence directe sur l'utilisation de l'IA :

- **Les données déduites représentent une nouvelle collecte :** Dans sa décision de novembre 2022 (Val-des-Cerfs), la CAI a déterminé que lorsque l'IA génère des prédictions ou des déductions sur des personnes (par exemple, prédire le risque de rotation du personnel ou déduire le revenu des clients), cela constitue une nouvelle collecte de renseignements personnels, déclenchant toutes les exigences applicables en matière de confidentialité.
- **Un examen humain significatif est nécessaire :** pour qu'une décision ne soit pas considérée comme « exclusivement automatisée », l'examen humain doit être substantiel et ne pas se limiter à approuver une suggestion de l'IA sans analyse critique.

La situation actuelle au niveau fédéral

Le Canada ne dispose actuellement d'aucune loi-cadre fédérale spécifique à l'intelligence artificielle. Le projet de loi C-27, qui intégrait la Loi sur l'intelligence artificielle et les données (LIAD), est devenu caduc à la suite de la prorogation du Parlement le 6 janvier 2025. Malgré l'absence de cette législation ciblée, d'autres cadres réglementaires s'appliquent :

- **La LPRPDE demeure en vigueur :** La Loi sur la protection des renseignements personnels et les documents électroniques s'applique aux activités commerciales du secteur privé sous réglementation fédérale, ou dans les provinces qui ne disposent pas d'une législation essentiellement similaire.
- **Principes conjoints des Commissaires à la protection de la vie privée :** En décembre 2023, les Commissaires à la protection de la vie privée du fédéral, des provinces et des territoires ont publié des principes conjoints sur l'IA générative. Bien qu'ils ne soient pas techniquement contraignants, ces principes constituent des orientations faisant autorité quant aux attentes en matière de conformité.
- **Code de conduite volontaire :** Le gouvernement fédéral maintient un code de conduite volontaire pour les systèmes avancés d'IA générative (septembre 2023).

Responsabilité malgré l'absence de lois spécifiques à l'IA

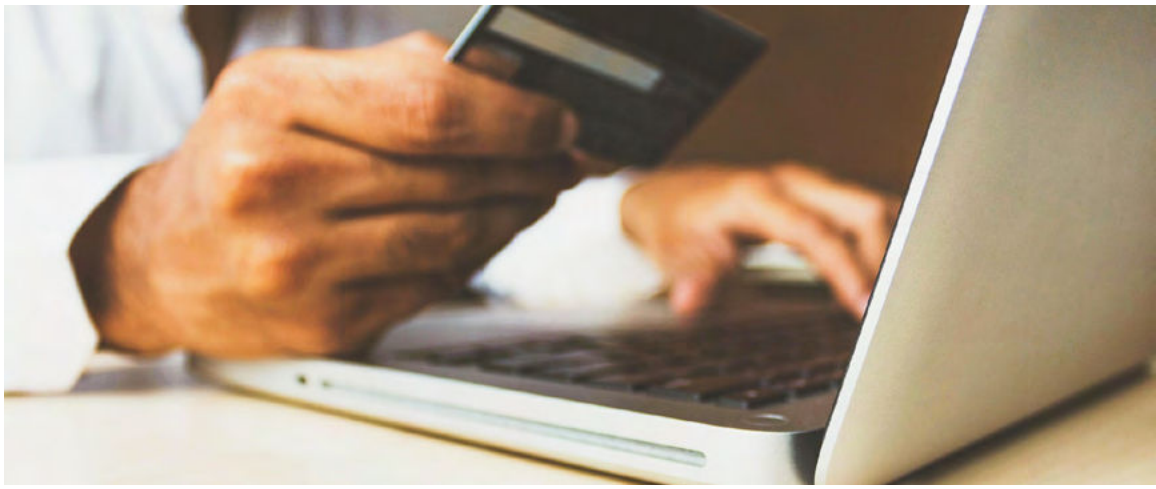
Même en l'absence de législation spécifique à l'IA, la responsabilité pour les préjudices liés à l'IA peut être engagée par le biais des mécanismes suivants :

- **Responsabilité civile et droit de la responsabilité délictuelle :** négligence ou déclaration inexacte faite par négligence (comme dans l'affaire Air Canada);
- **Obligations contractuelles :** violation de la confidentialité ou non-respect des niveaux de service convenus;
- **Lois sur la protection de la vie privée :** violations de la Loi 25, de la LPRPDE ou des autres lois provinciales sur la protection de la vie privée;
- **Loi sur les droits de la personne :** discrimination résultant de résultats biaisés ou de préjugés algorithmiques;
- **Obligations professionnelles :** manquements pour les professionnels régis par un ordre (avocats, comptables, professionnels de la santé, etc.).

Cadres internationaux de référence

Bien qu'ils ne soient pas directement contraignants au Canada, ces cadres fournissent des informations sur les meilleures pratiques et peuvent s'appliquer aux organisations ayant des activités internationales :

- **Loi européenne sur l'IA :** en vigueur depuis août 2024, avec une application complète prévue d'ici août 2026. Sa portée extraterritoriale peut toucher les organisations canadiennes desservant des clients dans l'Union européenne.
- **Cadre de gestion des risques liés à l'IA du NIST :** cadre volontaire élaboré par les États-Unis, désormais largement adopté à l'échelle internationale comme outil de gouvernance de référence.
- **ISO/CEI 42001:2023 :** première norme internationale certifiable portant sur les systèmes de gestion de l'intelligence artificielle au sein des organisations.



CLASSIFICATION DES RISQUES ET PROTECTION DES DONNÉES

Catégorisation des données pour l'utilisation de l'IA

Avant d'utiliser un outil d'IA, classez les données que vous comptez saisir. Cela déterminera les outils que vous pouvez utiliser et les autorisations requises.

NIVEAU	EXEMPLES	OUTIL D'IA AUTORISÉ
Restreint	Numéros d'identification fiscale, dossiers médicaux, cartes de crédit, données biométriques, données relatives aux enfants, mots de passe.	⚠ **Ne JAMAIS partager ces informations avec un outil d'IA**
Confidentiel	Secrets commerciaux, dossiers financiers, questions juridiques, dossiers RH, détails des dossiers clients.	Utilisation autorisée uniquement avec des outils d'entreprise ayant fait l'objet d'une EFVP complétée. Ne jamais utiliser d'outils publics.
Interne	Projets de documents internes, notes de réunion (anonymisées), procédures générales.	Utilisation autorisée avec les outils d'entreprise approuvés. Pour les outils publics, l'utilisation est permise uniquement si les données sont rigoureusement anonymisées au préalable.
Public	Documents publiés, informations publiques, questions de recherche générales.	Tout outil approuvé par l'organisation peut être utilisé.

Aide-mémoire décisionnel : Si X, alors Y

Utilisez ce cadre simple avant d'utiliser un outil d'IA :

SI ceci est vrai...	ALORS faites ceci
Les données contiennent des noms, des numéros d'assurance sociale, des informations médicales ou permettent d'identifier quelqu'un.	⚠ **NE les saisissez PAS dans un outil d'IA public. Point final.**
Le résultat sera utilisé pour prendre une décision ayant une incidence sur les droits, les avantages sociaux ou l'emploi d'une personne.	Exigez un examen approfondi par un être humain. Documentez la décision prise par l'être humain.
Le résultat sera partagé en externe (clients, public, partenaires).	Vérifiez tous les faits de manière indépendante. Faites approuver les résultats par une personne qualifiée avant leur publication.
Vous souhaitez utiliser un nouvel outil d'IA qui n'a pas encore été approuvé.	Soumettez une demande au responsable informatique/de la protection de la vie privée. N'utilisez aucun nouvel outil tant qu'il n'a pas été approuvé.
L'outil d'IA traitera des données à l'extérieur du Canada.	Une évaluation des facteurs relatifs à la vie privée est requise avant toute utilisation si des données personnelles sont utilisées (exigence de la Loi 25).

RÔLES ET RESPONSABILITÉS

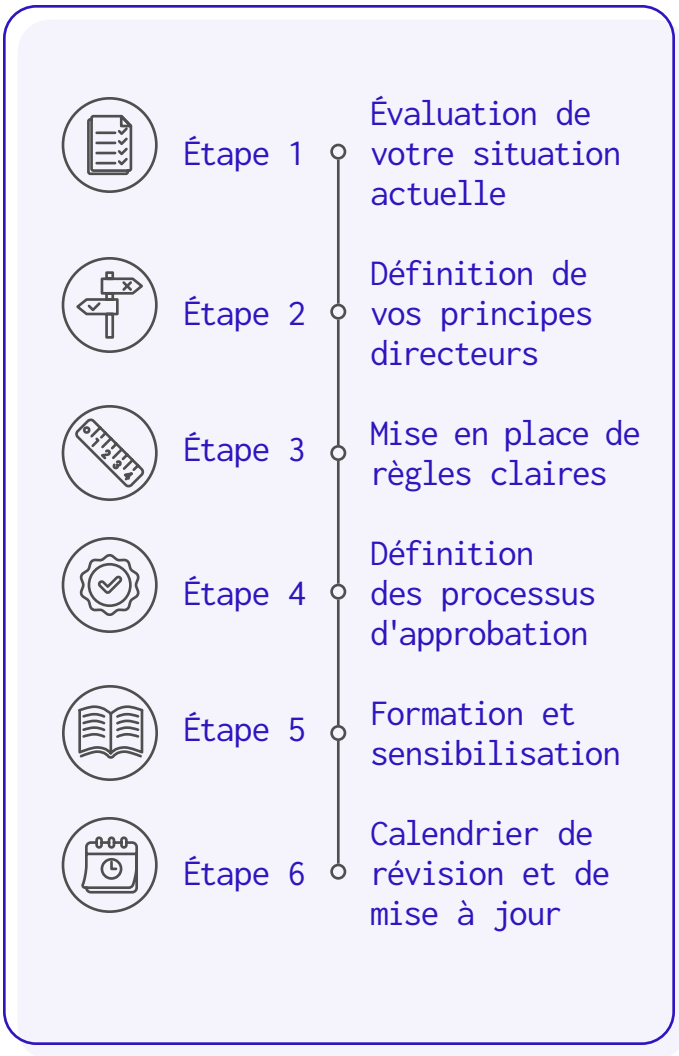
Une politique sans responsabilités claires est une politique qui prend la poussière. Dans les petites organisations, les rôles peuvent être combinés, mais l'essentiel demeure : chaque responsabilité doit être explicitement attribuée à une personne.

RÔLE	RESPONSABILITÉS	ATTRIBUTION
Dirigeant exécutif	Approuve la politique; rend compte au conseil d'administration; fait la promotion d'une utilisation responsable de l'IA.	Directeur général, PDG, directeur administratif... Dans le cas d'une municipalité, le maire.
Responsable de la protection des renseignements personnels	Veille au respect de la confidentialité; réalise les évaluations des facteurs relatifs à la vie privée; traite les demandes d'accès. Obligatoire en vertu de la Loi 25.	Par défaut : la personne ayant la plus haute autorité. Peut être délégué par écrit.
Responsable de la politique interne	Rédige et tient à jour la politique; coordonne les révisions périodiques; assure le suivi des mises à jour réglementaires.	Responsable des opérations, responsable informatique ou membre du personnel désigné.
Responsable informatique ou de la sécurité	Évalue les outils; gère la liste approuvée; surveille la sécurité	Fournisseur informatique externe ou personnel chargé des questions techniques
L'ensemble du personnel	Respecte la politique; vérifie les résultats; signale les problèmes; suit la formation	Tout le monde, y compris les sous-traitants et les bénévoles

Exigence de la Loi 25

Vous devez publier le titre et les coordonnées de votre responsable de la protection des renseignements personnels sur le site Web de votre organisation.

CRÉATION DE VOTRE POLITIQUE ÉTAPE PAR ÉTAPE



Étape 1 : Évaluation de votre situation actuelle

- Interrogez le personnel sur l'utilisation actuelle des outils d'IA (formelle ou informelle);
- Identifiez les outils déjà utilisés et leurs objectifs;
- Passez en revue les politiques existantes (confidentialité, informatique, ressources humaines, communications);
- Tenez compte de la sensibilité des données traitées par votre organisation.

Étape 2 : Définition de vos principes directeurs

Votre politique doit refléter les valeurs de votre organisation. Envisagez d'adopter des principes tels que :

1. **Le contrôle humain :** L'IA assiste mais ne remplace pas le jugement humain pour les décisions importantes.
2. **La protection de la vie privée :** Les renseignements personnels ne doivent jamais être saisis dans des outils d'IA publics.
3. **La vérification de l'exactitude :** Tous les résultats de l'IA doivent être vérifiés avant utilisation.
4. **La transparence :** Nous sommes transparents quant à l'utilisation des outils d'IA.
5. **La responsabilité :** Nous avons défini des responsabilités et un cadre clair pour la prise de décisions liées à l'IA.
6. **Non-discrimination :** L'utilisation de l'IA ne doit pas créer ou renforcer la discrimination.

Étape 3 : Mise en place de règles claires

Votre politique doit inclure des règles spécifiques dans les catégories suivantes :

Interdictions absolues

- La saisie de renseignements personnels dans des outils d'IA publics;
- L'utilisation de l'IA pour prendre des décisions finales concernant des individus sans examen humain;
- Le partage d'informations confidentielles sur l'organisation avec des outils d'IA non approuvés;
- La publication de contenu généré par l'IA sans révision ni approbation humaine;
- L'utilisation de l'IA pour l'analyse biométrique sans notification ni consentement de la CAI;
- L'utilisation de comptes personnels pour le travail organisationnel avec des outils d'IA;
- L'installation d'extensions de navigateur IA sans l'accord du service informatique.

Autorisations conditionnelles avec des mesures de protection

- L'utilisation de l'IA pour la rédaction, avec révision par un expert avant finalisation;
- L'utilisation d'outils d'IA approuvés par l'entreprise pour les tâches impliquant des données non sensibles;
- L'aide à la décision assistée par l'IA avec révision humaine documentée et décision finale.

Autorisations générales

- L'apprentissage de l'IA par la formation et l'expérimentation avec du contenu non sensible;
- L'utilisation de l'IA pour l'idéation et la recherche préliminaire;
- L'édition et la relecture de textes non confidentiels.

Étape 4 : Définition des processus d'approbation

NIVEAU DE RISQUE	EXEMPLES	APPROBATION	EXIGENCES
Faible	Brouillons internes, recherches, idéation.	Auto-approbation dans le cadre de la politique	Respecter la politique; vérifier les résultats
Moyen	Communications externes, demandes de nouveaux outils	Responsable de la politique	Utilisation du document; examen par des experts
Élevé 	Aide à la décision, déploiement de nouveaux systèmes d'IA, traitement de renseignements personnels.	Cadre de gouvernance supérieur et le responsable de la protection des renseignements personnels.	EFVP obligatoire; intervention humaine requise.

Étape 5 : Formation et sensibilisation

Une politique ne fonctionne que si les gens la comprennent. Celle-ci doit inclure :

- Une formation initiale lors du lancement de la politique;
- Une formation d'intégration pour les nouveaux employés;
- Des rappels annuels et mises à jour en cas de modification de la politique.

Étape 6 : Calendrier de révision et de mise à jour

L'IA générative évolue rapidement. Votre politique doit prévoir :

- Une révision formelle au moins tous les 12 mois (plus fréquemment la première année);
- Suivre les évolutions réglementaires de la CAI et des Commissaires à la protection de la vie privée;
- Numéro de version et date d'entrée en vigueur sur le document de politique.

EXEMPLES DE CLAUSES ET DE DIRECTIVES POUR VOTRE POLITIQUE

Adaptez ces modèles de déclarations à la réalité de votre organisation. Les éléments entre [crochets] doivent être personnalisés selon vos besoins spécifiques. N'hésitez pas à les bonifier pour mieux refléter votre culture interne.

Déclaration d'intention

> *« La présente politique établit des lignes directrices pour l'utilisation responsable des outils d'intelligence artificielle (IA) générative au sein de [nom de l'organisation]. Elle vise à tirer parti des avantages de ces outils en termes de productivité tout en protégeant la vie privée, en garantissant l'exactitude, en assurant la conformité juridique et en préservant la confiance du public. »*

Champ d'application

> *« Cette politique s'applique à tous les employés, sous-traitants, bénévoles et membres du conseil d'administration lorsqu'ils effectuent des tâches pour le compte de [nom de l'organisation]. Elle couvre tous les outils d'IA générative, qu'ils soient fournis par l'organisation ou accessibles à titre personnel, lorsqu'ils sont utilisés à des fins organisationnelles ou avec des données organisationnelles. »*

Interdiction relative aux renseignements personnels

> *« Les renseignements personnels ne doivent jamais être saisis dans des outils d'IA générative publics. Cela inclut les noms, les coordonnées, les détails des dossiers, les informations médicales, les informations financières ou toute autre information permettant d'identifier une personne. Cette interdiction s'applique que la personne soit un client, un membre, un employé ou un membre du public. Le non-respect de cette règle peut entraîner des mesures disciplinaires. »*

Supervision et responsabilité humaine

> *« Tout contenu généré par des outils d'IA doit être rigoureusement examiné par un membre du personnel qualifié avant toute utilisation officielle. L'employé ayant recours à l'outil demeure l'unique responsable de l'exactitude des résultats obtenus. Le contenu généré par l'IA ne doit en aucun cas constituer le seul fondement d'une décision ayant une incidence sur une personne. L'argument invoquant une "erreur de l'IA" ne constitue pas une justification acceptable en cas d'inexactitude ou de préjudice causé. »*

Prise de décision automatisée (conformité à la Loi 25)

> *« Toute utilisation de l'IA pour aider à prendre des décisions qui affectent les droits ou les intérêts des individus (par exemple, l'embauche, l'éligibilité à un service, l'évaluation des performances) doit inclure un examen humain significatif. La personne chargée de l'examen doit avoir l'autorité et la compétence nécessaires pour contester la suggestion de l'IA. Les individus ont le droit de savoir quand un traitement automatisé a été utilisé et de présenter leurs observations à un décideur humain. Cette exigence s'applique conformément à la Loi 25, section 12.1. »*

Outils approuvés

> *« Les outils d'IA suivants ont été approuvés pour une utilisation au sein de l'organisation : [liste des outils]. L'utilisation d'autres outils d'IA à des fins organisationnelles nécessite l'autorisation écrite de [fonction désignée]. La liste des outils approuvés sera révisée tous les trimestres. L'utilisation de comptes personnels ou de versions gratuites non approuvées d'outils d'IA pour le travail organisationnel est interdite. »*

Déclaration de transparence

> *« Sur demande, [nom de l'organisation] fera preuve de transparence quant à son utilisation des outils d'IA. Le contenu généré par l'IA qui interagit directement avec les clients ou le public (par exemple, les agents conversationnels) doit être clairement identifié comme automatisé au début de l'interaction. »*

RÉPONSE AUX INCIDENTS ET SIGNALEMENT

Votre politique doit inclure des procédures de gestion des incidents liés à l'intelligence artificielle.

Types d'incidents liés à l'intelligence artificielle

- **Exposition des données :** saisie d'informations confidentielles ou de renseignements personnels dans des outils d'IA publics non sécurisés;
- **Erreurs d'exactitude :** diffusion de renseignements erronés générés par l'IA ayant entraîné des actions préjudiciables ou une publication officielle.
- **Incidents liés aux biais et préjugés :** résultats produits par l'IA ayant mené à un traitement discriminatoire ou inéquitable envers des individus ou des groupes.
- **Incidents de cybersécurité :** accès non autorisé à des comptes d'IA, injection de requêtes malveillantes *(prompt injection)* ou détournement des systèmes.
- **Manquements à la politique :** utilisation d'outils d'IA non approuvés par l'organisation ou usage de l'IA pour des activités explicitement interdites.

Procédure de signalement

1. **Arrêtez immédiatement** l'activité qui a causé ou révélé l'incident;
2. **Documentez** ce qui s'est passé, quand, quelles données ont été concernées et quelles mesures ont été prises;
3. **Signalez l'incident** à votre supérieur hiérarchique et au responsable de la protection des renseignements personnels dans un délai de [X heures];
4. **Conservez** toutes les preuves (captures d'écran, journaux, enregistrements).

Obligation de notification selon la Loi 25

Si un incident de confidentialité impliquant des renseignements personnels présente un risque de préjudice grave, vous devez en informer le CAI et les personnes concernées. Conservez un registre de tous les incidents de confidentialité.

MISE EN ŒUVRE RAPIDE

Ne laissez pas la recherche de la perfection freiner vos progrès. Commencez par établir les bases de votre gouvernance et faites évoluer vos pratiques au rythme de la technologie.

Si vous disposez d'une journée

1. Envoyez un bref sondage pour demander quels outils d'IA le personnel utilise actuellement;
2. Communiquez une règle d'or : « Il est strictement interdit de saisir des renseignements personnels ou confidentiels dans des outils d'IA publics. »;
3. Identifiez la personne qui sera chargée d'élaborer une politique complète.

Si vous disposez d'une semaine

1. Remplissez la liste de contrôle d'auto-évaluation de la section 10;
2. Rédigez une politique de base en utilisant les exemples de la section 7;
3. Examinez-la avec votre responsable de la protection des renseignements personnels;
4. Obtenez l'approbation de la direction et communiquez la politique à l'ensemble du personnel.

Si vous disposez d'un mois

1. Réalisez un inventaire complet des outils d'IA dans l'ensemble de l'organisation;
2. Examinez les politiques existantes afin d'identifier les lacunes et les contradictions;
3. Élaborez une politique complète en tenant compte des commentaires des parties prenantes;
4. Créez une liste d'outils approuvés après avoir effectué une vérification préalable des fournisseurs;
5. Élaborez du matériel de formation et planifiez son déploiement;
6. Mettez en place des procédures de signalement des incidents.

Assurer une maintenance continue

1. Planifiez une révision régulière de la politique (les outils d'IA et les réglementations changent rapidement!);
2. Surveillez les mises à jour de la CAI et des Commissaires à la protection de la vie privée
3. Suivez les incidents et ajustez la politique en fonction des enseignements tirés
4. Intégrez la politique en matière d'IA dans l'intégration des nouveaux employés

À propos de Nord Ouvert

Renforcer la confiance dans les données, pour le bien commun

Nord Ouvert est une organisation à but non lucratif qui se consacre à l'avancement du bien commun. Aux côtés des gouvernements et des organisations à vocation civique de toutes tailles, nous fournissons une expertise en matière de données afin d'éclairer la prise de décision, de stimuler l'innovation, d'améliorer les services publics et les services offerts par la société civile, et de relever les défis les plus urgents de la société.

Notre travail consiste à renforcer la capacité des organisations, à prendre de meilleures décisions concernant la gestion de leurs données afin qu'elles soient utiles, exploitables, sécurisées et dignes de confiance tout au long de leur cycle de vie. Chez Nord Ouvert, nous combinons une expertise approfondie en matière de données avec une approche multidisciplinaire. Notre équipe est composée d'urbanistes, d'ingénieurs en logiciel, d'organisateurs communautaires, de scientifiques des données, de spécialistes en vérification cybernétique et des technologies de l'information, de sociologues, de géographes et de juristes spécialisés dans les technologies, ce qui nous permet d'apporter des perspectives diverses à chaque projet.

Nord Ouvert fait partie de Montréal en commun, un projet mené par la Ville de Montréal dans le cadre du Défi des villes intelligentes, réalisé avec le soutien financier du gouvernement du Canada.

opennorth.ca/fr

À propos du Défi des villes intelligentes et de Montréal en commun

Montréal en Commun est une communauté d'innovation pilotée par la Ville de Montréal dont les partenaires expérimentent des solutions en accès à l'alimentation, en mobilité et en réglementation municipale dans un désir de repenser la ville. Les projets sont mis en œuvre grâce au prix octroyé à la Ville de Montréal par le Gouvernement du Canada dans le cadre du Défi des villes intelligentes.

Auteur: Cristiano Therrien

Canada Montréal DÉFI DES VILLES INTELLIGENTES Montréal en commun

ANNEXES : LISTES DE CONTRÔLE ET RÉFÉRENCES

Annexe A - Liste de contrôle d'auto-évaluation

Utilisez cette liste de contrôle pour évaluer l'état de préparation de votre organisation. Cochez chaque élément auquel vous pouvez répondre « oui ».

Gouvernance et responsabilité

- ☐ Nous avons désigné une personne responsable de la gouvernance de l'IA
- ☐ Nous avons désigné un responsable de la protection des renseignements personnels (conformément à la Loi 25).
- ☐ L'équipe de direction a discuté de l'utilisation de l'IA générative
- ☐ Nous savons quels membres du personnel utilisent actuellement des outils d'IA

Politique et documentation

- ☐ Nous avons une politique ou des lignes directrices écrites sur l'utilisation de l'IA générative
- ☐ La politique énonce clairement ce qui est autorisé et ce qui ne l'est pas
- ☐ La politique traite des renseignements personnels dans les outils d'IA
- ☐ La politique exige un examen humain des résultats de l'IA
- ☐ La politique comporte une fréquence de révision et un numéro de version

Confidentialité et conformité juridique

- ☐ Nous avons examiné nos obligations en vertu de la Loi 25/LPRPDE
- ☐ Nous interdisons les renseignements personnels dans les outils d'IA publics
- ☐ Nous avons mis en place un processus d'évaluation d'impact sur la vie privée
- ☐ Nous savons où nos outils d'IA stockent et traitent les données

Sécurité et accès

- ☐ Nous disposons d'un inventaire des outils d'IA utilisés
- ☐ Nous contrôlons l'accès via des comptes organisationnels
- ☐ Nous avons examiné les conditions d'utilisation des outils d'IA que nous utilisons
- ☐ Nous avons mis en place des procédures de signalement des incidents

Qualité et vérification

- ☐ Nous exigeons une vérification humaine avant toute utilisation externe
- ☐ Nous interdisons l'utilisation de l'IA pour prendre des décisions sans supervision humaine
- ☐ Le personnel est sensibilisé aux risques d'hallucination de l'IA

Formation

- ☐ Le personnel a reçu une formation sur la politique en matière d'IA
- ☐ Le personnel sait à qui s'adresser en cas de questions

Interprétation des résultats

Si vous avez coché moins de 10 éléments, vous devez élaborer une politique complète. Si votre résultat se situe entre 10 et 15, vous disposez des bases nécessaires, bien que certaines lacunes importantes restent à combler. Si vous avez atteint 16 éléments ou plus, votre cadre est solide et vous pouvez vous concentrer sur l'amélioration continue.

Annexe B – Grille de vérification pour la diligence raisonnable des fournisseurs

Avant d'adopter un nouvel outil d'IA, posez-vous les questions suivantes et réfléchissez aux réponses :

1. Où les données sont-elles stockées et traitées? Le fournisseur peut-il garantir un hébergement au Canada ou au Québec?
2. Nos données seront-elles utilisées pour entraîner un modèle d'IA?
3. Quelles certifications de sécurité le fournisseur possède-t-il (SOC 2, ISO 27001)?
4. Combien de temps les données sont-elles conservées? Pouvons-nous les supprimer?
5. Quelles sont les obligations en matière de notification des incidents?
6. Le fournisseur a-t-il souscrit une assurance contre la cyber-responsabilité?

Consultez les **guides sur la confidentialité et la cybersécurité** de Nord Ouvert pour plus d'informations.

Références

Directives réglementaires canadiennes

- Commission d'accès à l'information du Québec (CAI)
- Commissariat à la protection de la vie privée du Canada - priv.gc.ca
- Guide du gouvernement du Canada sur l'utilisation de l'IA générative
- Directive sur la prise de décisions automatisée (gouvernement du Canada)

Cadres internationaux

- Principes de l'OCDE en matière d'IA;
- Recommandation de l'UNESCO sur l'éthique de l'IA;
- ISO/IEC 42001:2023;
- Cadre de gestion des risques liés à l'IA du NIST.

Ressources de Nord Ouvert

- Principes et pratiques en matière de protection des renseignements personnels - un guide de Nord Ouvert sur les exigences du Québec en matière de protection de la vie privée.
- La cybersécurité pour les petites et moyennes organisations - un guide de Nord Ouvert sur les principes fondamentaux de la cybersécurité.
- Politique de confidentialité des données : comment rédiger un projet complet - un guide de Nord Ouvert sur l'élaboration d'une politique de confidentialité solide.

L’IA générative dans votre organisation