POLITIQUE DES USAGES RESPONSABLES DE L'INTELLIGENCE ARTIFICIELLE

Adoptée : 2 février 2026

Résolution: 2026-02-XXX

Table des matières

1. Mise en contexte

L'intelligence artificielle (IA) est un domaine technologique émergent qui promet d'améliorer considérablement notre efficacité organisationnelle, tout en offrant de nouvelles occasions favorisant l'innovation et le développement. La Ville de Bromont (Ville) reconnaît l'impact structurant que IA exerce sur l'évolution des services municipaux, les façons de travailler et la relation avec la collectivité. L'IA est avant tout un outil d'aide à la décision : elle complète l'expertise des employées, employés, citoyennes et citoyens, sans se substituer à la valeur, au jugement et à la créativité humaine qui demeurent essentiels dans toute analyse ou prestation de service.

La présente Politique des usages responsables de l'intelligence artificielle (Politique) vise à encadrer l'utilisation responsable, éthique et durable de l'IA.

2. Objectifs

- **Fournir un cadre uniforme et accessible à l'ensemble des usagers**, en s'appuyant sur la présente Politique, un guide d'utilisation interne et une procédure Oups-IA pour assurer une compréhension et une application harmonisées.
- **Moderniser le fonctionnement municipal en automatisant les tâches répétitives** afin de permettre au personnel de se concentrer sur des missions à forte valeur ajoutée, tout en améliorant la qualité et l'efficacité des services offerts aux citoyennes et aux citoyens.
- **Promouvoir le développement d'un milieu de vie intelligent, innovant et durable**, où chaque direction exploite des solutions d'IA sur mesure, renforçant ainsi la culture numérique pour tous.
- **Assurer la protection des personnes et des groupes** en garantissant la confidentialité, la sécurité des renseignements, la transparence des algorithmes, ainsi qu'une utilisation éthique et responsable de l'IA.
- **Accompagner et former chaque usager du personnel municipal** dans la compréhension des avantages, des limites et des obligations liés à l'IA.
- **Encadrer et limiter la responsabilité de la Ville** en cas d'usage externe de l'IA afin d'assurer un usage sécurisé, conforme et de prévenir les risques d'utilisation inappropriée ou d'interprétations erronées des contenus générés.

3. Définitions et portée

Cette partie définit les notions centrales reliées à l'IA et précise l'étendue d'application de la Politique pour garantir une compréhension commune, une gouvernance responsable et l'inclusion de tous les usagers, qu'ils soient internes ou externes.

a. Définitions

Biais algorithmique : Tendance prédictive ou générative non désirée d'un système d'IA à favoriser ou à défavoriser certains résultats plutôt que d'autres (OQLF – Lien).

Brèche de sécurité informatique liée à l'IA : Vulnérabilité informatique ayant permis une intrusion illicite dans un outil ou un système d'IA et pouvant entraîner le vol, la divulgation ou la destruction de données importantes pour une organisation (définition inspirée de l'OQLF – Lien).

Une brèche de sécurité informatique liée à l'IA ou un imprévu relié à l'IA est qualifié comme tout événement non planifié ayant un impact potentiel ou avéré sur :

- La confidentialité ou la sécurité des données ;
- L'intégrité des résultats fournis par l'outil ou le système IA de la municipalité (ex. : réponse incomplète, erronée, biaisée) ;
- L'expérience ou la réputation de l'organisation.

Cycle de vie d'un document : Ensemble des étapes que franchit un document (électronique ou non) et qui vont de sa conception à sa destruction, en passant par sa diffusion et son archivage. (OQLF – Lien)

- **Notions rattachées** (Selon la *Loi sur les Archives du Québec*) **:**
  - Document actif : un document qui est couramment utilisé à des fins administratives ou légales ;
  - Document semi-actif : un document qui est occasionnellement utilisé à des fins administratives ou légales ;
  - Document historique : un document qui n'est plus utilisé à des fins administratives ou légales, mais qui est conservé pour causes justificatives ultérieures en fonction du calendrier de conservation de la Ville.

Dépersonnalisation : Un renseignement personnel est dépersonnalisé lorsqu'il ne permet plus d'identifier la personne concernée, directement ou indirectement.

Donnée numérique gouvernementale : Les données numériques gouvernementales constituent un actif informationnel stratégique du patrimoine numérique du gouvernement du Québec. Leur mobilité et leur valorisation au sein de l'administration publique à des fins administratives ou de services publics, en tenant compte de leur nature, de leurs caractéristiques et des règles d'accès et de protection qui les régissent, sont d'intérêt gouvernemental.

Évaluation des facteurs relatifs à la vie privée (ÉFVP) : La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (A-2.1)* défini dans quel(s) cas la Ville doit procéder à une ÉFVP.

Extrait de l'article 63.5 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (A-2.1):*

> ***63.5.*** *Un organisme public doit procéder à une évaluation des facteurs relatifs à la vie privée de tout projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels. (..)*

Hallucination d'IA : Contenu incorrect, inapproprié ou fictif généré par une intelligence artificielle générative (IAG) et présenté comme factuel, comme si les informations étaient authentiques ou adéquates par rapport à la requête d'origine (OQLF – Lien).

Incident de confidentialité : Événement défini conformément à l'article 63.9 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (A-2.1), soit :

> *1° l'accès non autorisé par la loi à un renseignement personnel ;*
> *2° l'utilisation non autorisée par la loi d'un renseignement personnel ;*
> *3° la communication non autorisée par la loi d'un renseignement personnel ;*
> *4° la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.*

Procédure à suivre en cas d'incident de confidentialité (Extrait de l'article 63.8 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (A-2.1)*) :

> **63.8.** *Un organisme public qui a des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel qu'il détient doit prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent.*
>
> *Si l'incident présente un risque qu'un préjudice sérieux soit causé, l'organisme doit, avec diligence, aviser la Commission. Il doit également aviser toute personne dont un renseignement personnel est concerné par l'incident, à défaut de quoi la Commission peut lui ordonner de le faire. Il peut également aviser toute personne ou tout organisme susceptible de diminuer ce risque, en ne lui communiquant que les renseignements personnels nécessaires à cette fin sans le consentement de la personne concernée. Dans ce dernier cas, le responsable de la protection des renseignements personnels doit enregistrer la communication.*
>
> *Malgré le deuxième alinéa, une personne dont un renseignement personnel est concerné par l'incident n'a pas à être avisée tant que cela serait susceptible d'entraver une enquête faite par une personne ou par un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois. (...)*

Intelligence artificielle (IA) : La Ville retient la définition du Conseil sur l'IA de l'Organisation de coopération et de développement économiques (OCDE), soit un « système automatisé qui, pour des objectifs explicites ou implicites, déduit, à partir d'entrées reçues, comment générer des résultats en sortie, tels que des prévisions, des contenus, des recommandations ou des décisions, qui peuvent influer sur des environnements physiques ou virtuels. Différents systèmes d'IA présentent des degrés variables d'autonomie et d'adaptabilité après déploiement ».

L'IA est également un domaine d'étude permettant de concevoir des systèmes ou des machines capables de simuler certaines facultés cognitives humaines, telles que l'apprentissage, l'analyse, la compréhension, la résolution de problèmes ou la prise de décision. Sous certaines conditions, certaines méthodes d'IA permettent même d'égaler ou de dépasser les capacités humaines dans des domaines très précis.

L'IA se distingue notamment par deux caractéristiques : l'autonomie et l'adaptabilité. Elle permet à des systèmes d'exécuter des tâches précises dans des environnements complexes de manière autonome, sans guidage constant d'un humain. Grâce à l'apprentissage par l'expérience, elle peut améliorer ses performances et s'adapter à de nouvelles situations afin de résoudre des problèmes variés, de plus en plus complexes.

IA générative (IAG) : Un type d'IA qui génère du nouveau contenu en modélisant les caractéristiques des données tirées des grands jeux de données qui alimentent le modèle. Alors que les systèmes d'IA traditionnels peuvent reconnaître les modèles ou classifier le contenu existant, l'IA générative peut créer du contenu unique sous plusieurs formes, comme du texte, une image, un fichier audio ou du code logiciel. (*Série de sensibilisation, Gouvernement du Canada, ITSAP.00.041)*

IA responsable : Approche visant à garantir que la responsabilité socioenvironnementale est prise en compte à toutes les étapes du développement et de la gouvernance de l'IA, afin de prévenir les préjudices et les injustices et d'orienter son développement vers des bénéfices durables dans un monde interconnecté.

Journaux conversationnels (logs) : Ce sont les historiques de requêtes (prompts) engagés entre l'usager et l'outil ou le système d'IA.

Outil ou système d'IA : Application, plateforme, service ou module intégrant un ou plusieurs systèmes d'IAG, capable d'analyser, de générer ou de recommander des données, des contenus ou des décisions. Cela inclut notamment les agents conversationnels ainsi que les outils d'automatisation, d'analyse de données, de prédiction ou de recommandation.

Renseignement personnel : Toute information concernant une personne physique permettant de l'identifier, directement ou indirectement, au sens de l'article 54 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*.

Usagers externes : Citoyennes, citoyens, partenaires, prestataires de services ou toute autre personne externe interagissant avec un outil ou un système d'IA offrant un résultat ou une interface mise à disposition par la Ville.

Usagers internes : Employés, employés, élues, élus, mandataires ou bénévoles de la Ville, utilisant un outil ou un système d'IA dans le cadre de leurs fonctions.

b. Portée

Cette Politique s'applique à tout usage, interne ou externe, d'un outil, d'un service, d'une interface ou d'un résultat généré par un système d'IA fourni, opéré ou validé par la Ville, notamment :

- À tous les secteurs d'activité municipaux utilisant l'IA — que ce soit à des fins de service à la population, administratives, de gestion, d'analyse de données, de consultation publique ou d'interaction avec les citoyennes et les citoyens ;
- À l'ensemble des données et contenus traités, analysés, générés ou recommandés par ces outils ou systèmes d'IA, qu'ils concernent des processus internes ou des services publics ;
- Aux obligations, responsabilités, comportements et limites imposés à tous les usagers internes et externes dans le respect des lois, des valeurs éthiques et des meilleures pratiques d'IA responsable.

4. Lois et cadre légal applicables

La présente Politique s'inspire des lois, règlements, arrêtés, décrets et orientations gouvernementales, notamment :

- La *Charte des droits et libertés de la personne* (Québec), notamment les principes d'égalité, de dignité, de protection contre la discrimination et de respect des droits fondamentaux ;
- L'*Arrêté ministériel no 2025-02 du ministre de la Cybersécurité et du Numérique* (publié le 3 décembre 2025) relatif à l'utilisation responsable de l'IA au sein des organismes publics ;
- Le *décret G-1.03*, incluant ses sections I et II portant sur la gouvernance et la gestion responsable des ressources informationnelles des organismes publics ;
- La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* ;
- L'*Énoncé de principes pour une utilisation responsable de l'intelligence artificielle par les organismes publics* ;
- La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, c. A-2.1) ;
- La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (dite « Loi 25 ») ;
- *Loi sur les archives* du Québec.

La Ville s'engage à modifier la présente Politique en fonction de l'évolution de l'encadrement légal de l'IA.

5. Principes directeurs de l'IA responsable

Les principes directeurs assurent que l'IA utilisée ou déployée par la Ville est alignée avec les valeurs d'équité, d'éthique, de transparence et de responsabilité sociale. De plus, elle s'appuie sur l'*Arrêté ministériel no 2025-02 du ministre de la Cybersécurité et du Numérique*. Elle s'assure de considérer le principe de proportionnalité qui propose de maintenir une réflexion proportionnelle aux risques encourus et aux bénéfices recherchés dans une démarche de mise en œuvre de tous outils ou systèmes d'IA au sein de la Ville. Enfin, l'IA responsable protège la primauté du jugement humain face à l'entièreté du cycle de vie des requêtes générées par l'IA.

On entend par cycle de vie de l'outil ou du système d'IA les phases suivantes:

- ☐ La phase de planification et de conception ;
- ☐ La phase de collecte et de traitement des données ;
- ☐ La phase de construction du modèle concerné ou l'adaptation d'un modèle existant pour des tâches spécifiques ;
- ☐ La phase de test ;
- ☐ La phase d'évaluation ;
- ☐ La phase de vérification ;
- ☐ La phase de validation ;
- ☐ La phase de mise à disposition pour son utilisation ;
- ☐ La phase d'exploitation et de suivi ;
- ☐ La phase de mise hors service.

(1) Primauté du jugement et de la responsabilité humaine : L'IA à la Ville est avant tout un outil d'aide à la décision, aide à la rédaction et au traitement des données : elle appuie l'expertise, la réflexion et la créativité humaine sans jamais s'y substituer. Les usages de nature plus autonome de l'IA, devront justifier de dispositifs techniques et organisationnels assurant la supervision humaine.

(2) Respect de la vie privée, des droits et de la sécurité : La confidentialité, la sécurité des données et les droits fondamentaux des personnes répondent aux standards et exigences légales. Toute collecte de renseignement est limitée au strict nécessaire, tel que le requière la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1). La Ville possède un *cadre de gouvernance* à l'égard des renseignements personnels tout au long du cycle de vie de ces renseignements, afin d'assurer leur collecte, utilisation, communication, conservation et destruction dans les règles.

(3) Gestion proactive des risques et de la conformité : Avant tout nouveau déploiement d'outils ou de systèmes IA, une évaluation systématique des risques (ex: biais, sécurité, confidentialité, conséquences sociales) est réalisée et documentée. L'ensemble des usages se conforme aux lois, règlements et meilleures pratiques applicables, notamment le fait de procéder à une ÉFVP. De plus, la Ville oblige

certaines pratiques de sécurité, tel que la dépersonnalisation afin de minimiser les risques dans le traitement de l'information dans les outils ou systèmes d'IA.

(4) Transparence, compréhension et traçabilité : Les modalités de fonctionnement, les limites et les impacts des systèmes d'IA sont rendus accessibles et compréhensibles à tous les usagers internes ou externes. La Ville favorise la transparence lorsque l'IA est utilisée de manière significative. Lorsque pertinent, notamment pour des communications publiques, des documents décisionnels, des recommandations officielles, des contenus destinés aux citoyennes et citoyen, ou des processus ayant un impact sur des droits, la Ville :

a. Suggère fortement aux usagers de l'IA à la transparence et à indiquer s'ils ont eu recours à l'IA dans l'exercice de leur fonction en ajoutant, la **mention « IA responsable »** dans leur production documentaire, ainsi que dans les métadonnées documentaires : *« Ce document a été réalisé et piloté par la Direction xxxx et propulsé par l'intelligence artificielle ».* Toutes les productions issues de l'outil ou système d'IA de la Ville sont systématiquement relues, validées et, au besoin, ajustées par un usager interne avant leur diffusion ou leur utilisation finale, afin d'assurer leur exactitude, leur conformité et leur adéquation au contexte local;
b. A Créé un logo qui doit être apposé graphiquement sur les documents qui ont utilisé l'IAG, lorsque la mention en a. y figure.

(5) Équité, inclusion et non-discrimination : La Ville s'engage à déployer et utiliser l'IA de manière équitable, respectueuse de la diversité et accessible à toute la collectivité. Les biais, discriminations ou effets indésirables doivent être identifiés, signalés et corrigés proactivement. Aussi, la Ville veille à mettre en place des dispositifs qui minimiseront les risques et les inconvénients reliés aux nouveautés technologiques pour maintenir l'actuel niveau d'accès à ses services auprès de ses citoyennes et citoyens. De plus, la Ville s'assure de prévenir la fracture numérique en offrant l'accompagnement nécessaire à ses équipes lorsqu'il est question de transformation organisationnelle des métiers par via les avancées technologiques.

(6) Souveraineté numérique : La Ville privilégie des solutions d'IA qui permettent la maîtrise des données, des accès et des infrastructures et qui s'alignent sur les orientations gouvernementales applicables. Dans la mesure du possible et selon une analyse de risques documentée, la Ville favorise:

a. L'hébergement au Québec ou dans une juridiction offrant un niveau de protection adéquat ;
b. La limitation des transferts de données hors Québec ;
c. La transparence sur la chaîne de sous-traitance (hébergement, infonuagique, services de soutien, sous-processeurs) ;
d. Des mécanismes permettant à la Ville de conserver un contrôle effectif sur les accès, la conservation et la destruction des données.

(7) Principe de l'efficience, de l'efficacité et de la pertinence : Dans l'ensemble de son cycle d'utilisation des outils et systèmes d'IA, la Ville poursuit l'objectif d'offrir à ses citoyennes et citoyens des services publics simplifiés, intégrés et de qualité.

(8) Principe de fiabilité et de robustesse : La Ville exige que ses systèmes et outils liés à l'IA soient fiables et robustes. Un dispositif de supervision encadre les usages et permet notamment de réaliser les vérifications nécessaires afin d'attester de la qualité des données traitées dans les outils ou systèmes d'IA.

(9) Principe de durabilité évolutive : L'utilisation responsable des outils ou des systèmes d'IA doit s'inscrire dans la recherche d'un développement durable. Concrètement, la Ville sera attentive à suivre les systèmes d'évaluation des impacts environnementaux des usages de l'IA au sein de son organisation.

(10) Dialogue, droit de regard, recours et correction : Tout usager interne ou externe peut interroger l'IA, demander de l'information, signaler une hallucination d'IA et/ou un biais algorithmique, demander une correction ou s'opposer à une décision prise ou appuyée par l'IA. Des mécanismes de recours, d'ajustement et de suppression de données sont notamment mis à disposition des usagers internes.

6. Gouvernance et responsabilité

La Politique définie les rôles et responsabilités pour assurer un suivi rigoureux, une réactivité en cas de problème et une évolution continue des pratiques, tant pour les applications internes, que certaines applications externes. La Ville reconnaît que la gouvernance et les usages de l'IA recoupent plusieurs

domaines de l'organisation et maintiendra la Politique évolutive afin de s'ajuster à l'évolution rapide des outils et systèmes d'IA.

6.1 Comité interne sur l'intelligence artificielle (ComitIA)

- Le ComitIA joue un rôle de consultation et d'ouverture pour tout projet pilote, idée créative ou démarche d'innovation qui pourrait leur être suggéré tant par les citoyennes et citoyens que les équipes municipales. Également, le ComitIA évalue et peut recommander l'intégration de nouveaux outils ou usages de l'IA au sein de la Ville ;
- Collabore avec le responsable de la protection des renseignements personnels (RPRP) et le Comité sur la protection des renseignements personnels de la Ville sur l'accès à l'information et la protection des renseignements personnels (Comité AIPRP) pour le traitement des ÉFVP ;
- Assiste le référant IA à la réalisation de la démarche de gestion de risques ;
- Documente statistiquement les usages et analyse les impacts des outils et systèmes d'IA via un espace partagé à l'interne, propose des ajustements et s'assure de l'alignement avec l'éthique, les lois et la stratégie municipale ;
- S'assure que l'ensemble des principes d'usage de l'IA responsable soient respectés dans un calendrier opérationnel des tâches liées à l'exécution des dispositifs de supervision des usages liés aux outils et/ou aux systèmes d'IA ;
- Confirme la faisabilité technique, les contrôles de sécurité et la capacité de journalisation/traçabilité quant aux outils et aux systèmes d'IA utilisés par la Ville ;
- Diffuse une fois par année une actualité citoyenne pour informer les Bromontois(es) sur l'évolution des usages de l'IA dans leur municipalité ;
- Coordonne la formation continue et la sensibilisation des usagers internes et, au besoin, des usagers externes ;
- Le ComitIA est composé des titulaires des postes suivants qui se réunit minimalement deux fois par année:
    - Un(e) représentant(e) de la Direction générale ;
    - Un(e) représentant(e) de la Direction du service du greffe et des affaires juridiques, autre que le RPRP ;
    - Un(e) représentant(e) de la division technologie de l'information de la Direction des services administratifs et soutien à l'organisation ;
    - Un(e) représentant(e) de la Direction de la gestion des actifs et des grands projets ;
    - Un(e) représentant(e) de la Direction de la gestion durable du territoire ;
    - Un(e) représentant(e) de la Direction de la sécurité publique ;
    - Un(e) représentant(e) de la Direction des relations avec la communauté et de l'expérience citoyenne ;
    - Un(e) représentant(e) de la division des ressources humaines et du développement organisationnel de la Direction des services administratifs et soutien à l'organisation ;

6.2. Référent IA

- Préside le ComitIA et doit nommer un/e secrétaire dans le groupe afin de prévoir les dates de rencontre du ComitIA ;
- Est responsable de la démarche de la gestion des risques ;
- Est responsable des redditions de compte, tant interne qu'externe et de faire des recommandations d'amélioration (gouvernance, sécurité, documentation, processus). En complément de l'audit externe annuel, la Ville peut réaliser des audits internes périodiques ciblés (par échantillonnage ou par secteurs à risque) afin de vérifier l'application de la présente Politique et de renforcer l'amélioration continue ;
- Agit comme personne-ressource pour les usagers internes (et au besoin pour les usagers externes): soutien au quotidien, conseils pratiques, remontée rapide de toutes les possibles brèches de sécurité informatique, liées à l'IA ;
- Il tient à jour deux registres:
    - Le registre officiel des outils ou systèmes d'IA de la Ville ;
    - Le registre des brèches de sécurité informatique liées à l'IA.

6.3. Responsable de la protection des renseignements personnels (RPRP)

- Assure la conformité à la Loi 25 dans tous les traitements d'IA ;
- Reçoit et traite les demandes d'accès, de rectification et les plaintes relatives à la vie privée et les incidents de confidentialité au sens de l'article 63.8 de la Loi sur l'accès à l'information ;

- Assume et encadre la réalisation des ÉFVP en collaboration avec le Comité AIPRP;
- Est responsable du traitement des incidents de confidentialité.

6.4. Division des technologies de l'information (TI)

- Assure la sécurité, la robustesse et la conformité technique des outils et le système d'IA ;
- Mets en place les contrôles d'accès et la surveillance des brèches d'informations et d'usages ;
- Soutiens les usagers internes dans le maintien et l'évolution des systèmes : gestion quotidienne, mises à jour, réponse aux brèches d'informations et d'usages et conformité réglementaire.

6.5. Direction générale et directions

- Valident l'utilisation de l'IA dans les diverses directions: s'assurent de l'intégration éthique de la cohérence avec les valeurs municipales et du respect de la Politique de façon globale ;
- Autorise le déploiement et accepte explicitement le niveau de risque résiduel, lorsque applicable, sur la base d'une documentation écrite ;
- Jouent un rôle clé dans la remontée et le traitement des problèmes ou recommandations des directions.

6.6. Usagers

- S'informe sur les bonnes pratiques, les limites et les obligations en consultant les différentes *Politiques de la Ville ;*
- Signale toute situation suspecte, erreur, hallucination d'IA, biais algorithmique, brèche de sécurité d'information ou usage non conforme au référent IA et incident de confidentialité ;
- Applique le principe de validation humaine et d'esprit critique avant toute prise de décision importante basée sur l'IA ;
- Respecte les procédures d'accès, de confidentialité et de sécurité des données.

7. Choix d'outil ou système d'IA

Seuls les outils ou systèmes d'IA ayant été préalablement autorisés selon les paramètres de la présente Politique peuvent être utilisés par les usagers internes et pour les usages destinés aux citoyennes et citoyens.

Le choix d'un outil ou système d'IA est fondé sur les axes de priorités suivants, notamment :

Gestion de risques :

Toute utilisation d'un outil ou système d'IA repose sur une démarche de gestion des risques exhaustive, par le référant IA et assisté par le ComitIA, comprenant minimalement les étapes suivantes :

- Identifier tous les risques organisationnels liés à l'outil ou système d'IA (éthique, sécurité de l'information, gouvernance des données, juridique, réputation, impacts sociaux, etc.) ;
- Analyser les risques (causes, conséquences, scénarios plausibles) ;
- Évaluer les risques et prioriser leur traitement ;
- Déterminer les mesures de mitigation, les responsables et les échéances ;
- Approuver les résultats de l'analyse des risques et la décision de déploiement ;
- Assurer le suivi et la revue périodique des risques selon la fréquence déterminée par le niveau de risque et l'évolution du contexte.

Sécurité et respect de la vie privée :

- Protection des renseignements personnels et des informations confidentielles et sensibles : L'outil doit être développé et configuré pour respecter les exigences légales en matière de protection des renseignements personnels. Le système intègre des contrôles d'accès stricts, assure la traçabilité des usages, de conservation des usages et des limites de diffusion de ses données et dépersonnaliser celles-ci lorsque requis ;
- Traçabilité du cycle de vie des données encodées dans le système d'IA : Modalités de conservation, destruction et purge des données et métadonnées. Obligations de journalisation, traçabilité et accès aux informations nécessaires à un audit ;

- L’obligation de notification en cas de reconnaissance d’entrées de renseignements personnels et d’informations confidentielles ou sensibles ;
- Obligations de notification rapide en cas de brèche informatique de sécurité ou d’incident de confidentialité ;
- Droits de vérification/audits raisonnables par la Ville, selon le niveau de risque et les obligations applicables ;
- Exigences de localisation/hébergement : les serveurs de l’outil ou du système d’IA doivent être à 100% hébergés minimalement au Canada et de manière privilégiée au Québec ;
- Analyse des risques (incluant ÉFVP, sécurité, éthique, juridique, gouvernance) ;
- Maîtrise des risques et de l’innovation : le choix de l’outil doit réduire les risques d’introduction de biais non contrôlés, de fuites de données ou d’utilisation d’outils inadaptés, tout en permettant à la Ville d’explorer les bénéfices de l’IA dans un cadre maîtrisé et évolutif ;
- Suppression définitive des données suivant une éventuelle rupture d’entente avec un prestataire de service 30 jours suivants la fin du contrat ;

Respect de la souveraineté des données de la Ville :

- Capacité à réaliser une description d’un cas d’usage pour la Ville tant sur l’aspect des usages internes que des usages possibles externes (objectif, utilisateurs, impacts, périmètre) ;
- Propriété exclusive : La Ville demeure la seule propriétaire de tous les contenus générés par les outils ou systèmes d’IA autorisés et doit pouvoir décider de ses critères d’autorisation (ou refus) et conditions d’utilisation ;
- Engagement du prestataire de service du non-partage des informations : Engagement écrit relatif au non-entraînement des modèles sur les données ou contenus de la Ville, sauf autorisation explicite ;
- Possibilité de faire des périodes de test en amont de l’entente contractuelle ;
- Transparence : L'outil doit assurer une information claire sur ses usages et limites ; chaque utilisateur interne ou externe est informé des modalités et des objectifs de l’utilisation de l’IA, avec possibilité de rétroaction ou de contestation lorsque pertinent ;

Valorisation de l’inclusion dans les usages :

- La pertinence municipale et conformité : L’outil ou le système d’IA doit être conçu pour s’adapter aux besoins spécifiques des municipalités, soutient la conformité légale à l’utilisation de l’IA ;
- Accessibilité et convivialité : L’outil doit permettre à l’ensemble des employées et employés de bénéficier d’un environnement intuitif et d’outils évolutifs (rédaction, synthèse, automatisation, soutien à la décision), tout en offrant, selon les modalités prévues, des fonctions accessibles aux citoyennes et aux citoyens pour certains services ou communications ;

Méthode d’évaluation :

- L’outil ou le système d’IA doit pouvoir autoriser des droits de vérification/audits raisonnables par la Ville, selon le niveau de risque et les obligations applicables ;
- Maîtrise des risques et de l’innovation : L’outil ou système d’IA doit réduire les risques d’introduction de biais non contrôlés, de fuites de données ou d’utilisation d’outils inadaptés, tout en permettant à la Ville d’explorer les bénéfices de l’IA dans un cadre maîtrisé et évolutif ;
- Offrir un plan de suivi des impacts avant et après déploiement ;
- Plan de mise hors service et exigences de purge/destruction/archivage.

7. Dispositifs de sécurité entourant les usages

7.1 Supervision humaine

- Les usagers internes doivent systématiquement valider leurs résultats générés par les outils ou les systèmes d’IA en relisant, évaluant et si nécessaire, en ajustant les suggestions et les contenus produits.

7.2 Principe de minimisation

- Les usagers internes n'utilisent que les informations nécessaires dans l'exercice de leur fonction, dans le respect des principes directeurs, à l'intérieur des outils et des systèmes d'IA (priorité aux métadonnées; éviter le contenu complet sauf nécessité justifiée) ;
- La conservation des journaux conversationnels est effectuée en minimisant le poids des données qui ont vocation à être conservées.

7.3 Dépersonnalisation et informations confidentielles ou sensibles

- Les usagers internes doivent dépersonnaliser les renseignements personnels avant de les intégrer dans des outils ou des systèmes d'IA, en retirant, à titre d'exemple :
  - Des informations financières ou hautement sensibles (ex.: numéros de cartes, informations bancaires) ;
  - Des identifiants gouvernementaux (ex.: NAS/NSS, numéros de permis/assurance) et autres identifiants uniques ;
  - Des informations médicales ;
  - Des informations concernant des mineurs ;
  - Des informations sensibles (évaluations disciplinaires nominatives, dossiers médicaux, etc.);
- Les usages internes doivent restreindre l'entrée d'informations confidentielles et/ou sensibles dans des outils ou des systèmes d'IA, en retirant, notamment, les secrets industriels, renseignements industriels ou des renseignements financiers, commerciaux, scientifiques ou techniques et les informations protégées par la notion du droit d'auteur.

7.4 Consentement

- Toute collecte et/ou utilisation de renseignements personnels, d'informations confidentielles et/ou sensibles par ou via un outil ou un système d'IA municipal sont soumises à un consentement clair et éclairé de l'usager.
- Toute utilisation d'un nouvel outil ou système d'IA ou traitement automatisé est précédé d'une communication claire aux usagers internes et externes impliqués ;
- Les citoyennes et les citoyens, les employées et employés, les prestataires de service sont systématiquement informés :
  - De la collecte et de l'utilisation de leurs renseignements personnels ;
  - De la finalité de l'utilisation, y compris si l'IA produit des décisions automatiques ou des recommandations ayant un impact significatif ;
  - De la possibilité de contester, demander l'accès, la rectification ou la suppression de leurs informations.

7.5 Robustesse proportionnelle

- Des mesures technologiques appropriées (contrôles d'accès, chiffrement, authentification forte, surveillance des accès) sont exigées pour protéger la confidentialité et l'intégrité des renseignements personnels et des informations confidentielles ou sensibles.
- En cas de brèches de sécurité informatique, la Ville applique une procédure interne nommée la « procédure OUPS-IA ». La procédure sert à consigner les brèches de sécurité informatiques liées à l'IA et à rétroagir sur l'événement afin que la Ville puisse s'améliorer en continue dans le traitement de ce type d'événement.
- En cas d'incident de confidentialité impliquant des renseignements personnels, la Ville applique la procédure à suivre dans la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*.

7.6 Exigences en matière de conservation des journaux conversationnels

Les conversations avec les outils ou systèmes d'IA sont considérées comme un document de travail. Lorsque disponible, la Ville privilégie:

- Les modes de conversation éphémères ou sans historique ;
- La suppression de conversations contenant des éléments sensibles ;

- Le classement des requêtes et conversations entrées avec l'IA.

7.7 Modalités de sauvegardes

(1) Par la Ville :

- Conserve l'historique général de l'ensemble des journaux conversationnels clairement défini et, idéalement, configurable, au même titre qu'un document dit actif pour une durée de la rétention minimale : 12 mois ;
- Veille à demander à chaque année à son/ses prestataire(s) de services les journaux conversationnels générés par les usagers ;
- Veille à conserver les journaux conversationnels comme document inactif en fonction du calendrier de conservation prescrit pour ce type de documentation ;
- Effectue des sauvegardes chiffrées, avec une durée de conservation qui est déterminée par son calendrier de conservation (la suppression pouvant être effective à l'expiration des cycles de sauvegardes) ;
- Assure que l'outil ou le système d'IA offre un hébergement et un chiffrement en transit et au repos conformes aux normes en vigueur ;
- Assure des contrôles d'accès (rôles, moindre privilège) et une traçabilité des accès administratifs (accès multi-facteurs, contrôle des rôles séparés par privilège).

(2) Par l'employée ou employé:

- Est responsable de documenter ses journaux conversationnels avec l'IA dans l'environnement de l'outil ou du système utilisé. Par la suite, l'employée ou l'employé doit les consigner dans le système d'archivage de la Ville selon le principe de minimisation et dans le respect des règles de gestion documentaire et du calendrier de conservation en vigueur ;
- Effectue la sauvegarde des journaux conversationnels (logs) en respectant le principe de minimisation.

7.8 Modalités de suppression

L'outil ou le système d'IA doit permettre une suppression possible par l'utilisateur et/ou l'administrateur, avec un délai de purge prescrit en fonction du calendrier de conservation des documents en vigueur :

- Sur le plan individuel, l'employée ou l'employé est responsable de ses propres suppressions lorsque le document est reconnu comme étant actif ;
- Pour tous les documents administratifs produits de nature semi-active ou encore inactive, le délai de purge suivra le cycle de vie dudit document ;
- Lorsque le document arrivera en fin de vie, il sera nécessaire de purger et supprimer les conversations liées à l'IA qui concernent le cycle de vie de ce document.

8. Limites de responsabilité

Malgré tous les efforts mis en place pour assurer la fiabilité, la sécurité et la pertinence des outils d'IA, il est important de rappeler :

- Que l'utilisation inappropriée, détournée ou non conforme des services, contenus ou résultats générés par l'outil ou le système d'IA relève de la responsabilité de l'usager interne ou externe ;
- Que certains contenus produits automatiquement ou semi automatiquement peuvent comporter des limites (erreurs, imprécisions, omissions, hallucinations), notamment lorsqu'ils n'ont pas été officiellement validés et publiés par la Ville ;
- **L'usager externe est responsable de toute utilisation qu'il fait des services ou contenus et doit s'assurer de respecter les lois applicables et la présente Politique. De plus, la Ville décline toute responsabilité pour les dommages résultant d'une utilisation des services ou contenus par un usager externe non conforme au cadre autorisé décrit à la présente Politique, dans la mesure où ces dommages découlent de cette utilisation non conforme ;**
- Aucune décision automatisée ayant un effet juridique, administratif, financier, disciplinaire ou portant atteinte à des droits ne peut être prise exclusivement sur la base d'un résultat généré par un outil ou un système d'IA. Dans ces situations, une intervention humaine est obligatoire et doit inclure, au minimum:

- La revue critique des informations produites par l'IA ;
- La validation des sources, données ou hypothèses pertinentes ;

La décision finale assumée par une personne dûment autorisée, conformément au cadre applicable de la Ville.

9. Formation et sensibilisation

Pour garantir une utilisation responsable, sécuritaire et innovante de l'IA, la Ville investit dans la formation continue, la veille technologique et la sensibilisation de ses équipes ainsi que, dans certaines mesures, les usagers externes.

9.1. Sensibilisation du public et des partenaires

- **Information accessible à tous :** Un guide d'utilisation interne est diffusé aux citoyennes et citoyens : il explique simplement ce qu'est l'IA municipale, les usages autorisés, les bonnes pratiques à adopter et les voies de recours. Ce guide est accessible en ligne et régulièrement mis à jour ;
- **Webinaires, ateliers et capsules de sensibilisation :** La Ville propose, ponctuellement ou selon les besoins, des séances d'information ouvertes à la population et aux partenaires pour démystifier l'IA, répondre aux questions et recueillir les préoccupations ;
- **Encouragement à la vigilance citoyenne** : Chacun est invité à signaler tout usage douteux, à poser des questions sur le fonctionnement de l'IA municipale ou à proposer des pistes d'amélioration.

9.2. Formation interne et sensibilisation

- **Formation obligatoire du personnel :** Tous employée et tout employé et/ou élue, élu, utilisant l'outil ou le système IA suit une formation obligatoire, notamment sur l'IA responsable, l'IA durable, ses possibilités, ses limites, la gestion des biais, la sécurité, la confidentialité et les procédures en cas de brèche de sécurité informatique ;
- **Sessions de mise à jour:** Des ateliers réguliers présentent les nouveautés, les bonnes pratiques, les exemples d'usage et les retours d'expérience – y compris les situations problématiques ou innovantes rencontrées à la Ville ou ailleurs ;
- **Accompagnement et mentorat :** Le référent IA se tient à disposition pour former, accompagner les nouveaux usagers et répondre aux questions du quotidien.

9.3 Veille technologique et amélioration continue

- **Veille sur les innovations et les normes :** Le ComitIA surveille les avancées en matière d'IA municipale, de réglementation, de sécurité ou d'éthique, afin de recommander/mettre à jour la Politique, les outils d'IA et les formations au besoin ;
- **Formation obligatoire :** Le référant IA doit s'assurer de recevoir des formations en lien avec toutes les nouveautés en termes d'encadrement sur l'IA ;
- **Intégration des meilleures pratiques :** Les retours d'expérience, les propositions des usagers internes et les bonnes pratiques observées dans d'autres municipalités servent à l'évolution continue de la gouvernance de l'IA à la Ville.

10. Ressources et outils internes

Liste non-exhaustive

- **Guide d'utilisation interne** : Document accessible aux usagers internes, résumant les usages acceptés, les bonnes pratiques, les procédures en cas de brèches de sécurité informatique. Disponible sur l'intranet municipal et sur le site web de la Ville ;
- **Procédures et formulaires** : Procédure OUPS-IA ;
- **Le registre officiel des outils ou systèmes d'IA** de la Ville ;
- **Le registre des brèches de sécurité informatique** liées à l'IA ;

- **Foire aux questions (FAQ) IA** : Réponses aux questions fréquentes sur l'utilisation de Munia, la sécurité, la confidentialité, les limitations et les droits des usagers ;
- **Coup d'œil de l'IA :** Document interne réservé à l'usage des équipes municipales ;
- **Coup d'œil de l'IA citoyens :** Document qui sera diffusé à l'externe.

11. Révision et évolution de la Politique

L'IA est un domaine en évolution rapide. La Ville s'engage à maintenir la présente Politique vivante, adaptée aux changements technologiques, réglementaires et aux besoins du personnel, des citoyennes et citoyens.

- **Révision périodique** : La présente Politique est réévaluée au moins une fois par année par le ComitIA (ou plus au besoin) ;
- **Signalement et participation** : Les usagers sont encouragés à transmettre leurs suggestions ou préoccupations au ComitIA, qui seront examinées lors des travaux de révision ;
- **Réalisation d'un audit annuel indépendant** : Afin de s'assurer que l'usage demeure neutre et en adéquation avec le cadre législatif, la Ville réalisera une fois par année un audit externe pour demeurer un opérateur d'IA qui est toujours actuel et indépendant.

12. Adoption

La présente Politique a été adoptée le 2 février 2026 par la résolution 2026-02-XXX.

Mention IA responsable : *« Ce document a été réalisé et piloté par la Ville de Bromont et propulsé par l'intelligence artificielle.* ***Mention IA responsable :*** *« Ce document a été réalisé et piloté par la Ville de Bromont et propulsé par l'intelligence artificielle. »*

ANNEXE A – NOS USAGES AUTORISÉS

À titre informatif, l'IA à la Ville peut être utilisée dans les contextes suivants :

Liste non exhaustive

- **Administration et gestion internes**
  - Rédaction de documents administratifs, de notes de service, d'ordres du jour et de comptes rendus de réunions ;
  - Génération de modèles de documents ou de courriels pour la communication interne et externe ;
  - Automatisation de processus répétitifs : gestion des rendez-vous, préparation de rapports, organisation de tâches, gestion documentaire ou suivi des demandes administratives ;
- **Soutien à la décision publique**
  - Analyse de données brutes (sondages, participation citoyenne, statistiques urbaines, données environnementales) pour aider à la prise de décision éclairée des gestionnaires et des élues et élus ;
  - Élaboration de synthèses, de visualisations, ou de scénarios prédictifs sur des enjeux municipaux tels que la planification urbanistique, la mobilité, l'aménagement du territoire ou la gestion de ressources ;
- **Gestion et optimisation des services municipaux**
  - Appui à la gestion de l'énergie, de l'eau, des déchets et autres ressources pour améliorer l'efficacité, la durabilité et le service à la population ;
  - Soutien à la sécurité publique, par exemple via l'analyse de tendances, la production de signalements anonymisés ou l'optimisation des interventions dans des contextes permises ;
- **Engagement citoyen et communication**
  - Préparation de réponses automatisées ou de suggestions de messages à destination des citoyennes et citoyens dans le cadre de demandes d'information, d'avis, de formulaires en ligne ou via des robots conversationnels/assistants virtuels ;
  - Production et diffusion de contenus informatifs adaptés (affiches, infolettres, FAQ) ;
- **Formation et développement organisationnel** :
  - Création de modules pédagogiques, de guide d'utilisation interne, de capsules d'information ou de questionnaires d'autoévaluation, sondages, analyse synthèse, création de gabarits, etc. à l'intention du personnel ou des usagers.