
TITRE : **POLITIQUE ENCADRANT L'UTILISATION DE L'INTELLIGENCE ARTIFICIELLE**

APPROUVE PAR: CONSEIL D'ADMINISTRATION

CODE : **C3-D117**

EN VIGUEUR : 27-01-2026

RES. : CA-810-9818
27-01-2026

RESPONSABILITE : SECRETARIAT GENERAL

REVISION PREVUE : 2029

TABLE DES MATIÈRES

1	PRÉAMBULE	2
2	OBJECTIFS	2
3	CADRE JURIDIQUE	2
4	CHAMP D'APPLICATION	3
5	DÉFINITIONS	3
6	RÔLES ET RESPONSABILITÉS	4
6.1	Secrétariat général	4
6.2	Personnel cadre	4
6.3	Personnes utilisatrices	4
6.4	Comité sur la sécurité de l'information et le Comité sur l'accès à l'information et sur la protection des renseignements personnels (CSI-CAIPRP)	4
6.5	Comités de réflexion	4
6.6	Comité conseil-IA	5
7	LIGNES DIRECTRICES	5
7.1	Respecter la vie privée	5
7.2	Respecter la confidentialité	5
7.3	Respecter les principes de droits d'auteur	5
7.4	Assurer la sécurité de l'information	5
7.5	Agir de façon responsable	6
7.6	Décisions fondées sur un processus automatisé	6
7.7	Autres considérations	6
7.8	Directives et indications d'application gouvernementales	7
8	RESPONSABLE DE L'APPLICATION	7
9	MISE À JOUR	7
10	ENTRÉE EN VIGUEUR	7

1 PRÉAMBULE

- a) Le déploiement des outils d'intelligence artificielle (IA) au sein d'une organisation comporte des enjeux importants, tant en matière de conformité légale que de gestion des risques opérationnels et éthiques. En tant que technologie émergente et complexe, l'IA soulève des questions relatives à la transparence, à la responsabilité, et à l'impact sur les êtres vivants et l'environnement. Ces questions pourraient exposer l'Université du Québec à Rimouski (Université) et les membres de la communauté universitaire à plusieurs risques, notamment en matière de protection de la vie privée et protection des renseignements personnels, de sécurité de l'information et de propriété intellectuelle.
- b) Pour réduire ces risques, l'Université désire adopter des lignes directrices pour guider les membres de la communauté dans leurs activités utilisant des outils d'IA. De plus, ces lignes directrices permettront à l'Université de se conformer au cadre légal et réglementaire.
- c) Cette politique n'établit pas de modalités spécifiques d'utilisation dans les contextes d'enseignement, d'étude ou de recherche.

2 OBJECTIFS

La présente politique poursuit les objectifs suivants :

- a) encadrer l'usage de l'intelligence artificielle (IA) au sein de l'Université en définissant des lignes directrices relatives au respect du cadre légal et réglementaire applicable; ces lignes directrices permettent d'établir les balises minimales nécessaires pour assurer la conformité aux lois en vigueur, notamment en matière de protection des renseignements personnels, de sécurité de l'information et de propriété intellectuelle;
- b) établir, en créant divers comités, un modèle de gouvernance en matière d'intégration et d'utilisation de l'intelligence artificielle à l'Université.

3 CADRE JURIDIQUE

La présente politique est élaborée en tenant compte du cadre juridique suivant :

- *Code civil du Québec* (RLRQ, c. CCQ-1991)
- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1)
- *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ, c. G-1.03)
- C3-D99 Politique de sécurité de l'information
- C3-D109 Cadre de gestion en sécurité de l'information
- C3-D111 Politique établissant le cadre de gouvernance en matière de protection des renseignements personnels
- C2-D112 Directive sur la collecte, l'utilisation et la communication des renseignements personnels
- Indication d'application IA-RI-2025-003-OP – Mesures applicables lors de l'utilisation de l'intelligence artificielle générative

4 CHAMP D'APPLICATION

Cette politique s'applique à toute la communauté universitaire.

5 DÉFINITIONS

Aux fins de la présente politique, les termes suivants se définissent comme suit :

Acquisition d'un outil d'intelligence artificielle: acheter, implanter, programmer, développer ou autrement obtenir une licence d'utilisation d'un outil d'intelligence artificielle.

Analyse de sécurité : analyse effectuée par l'équipe de sécurité du Service des technologies de l'information (STI) ayant pour objectif d'identifier les risques en matière de sécurité de l'information et de cybersécurité.

Analyse SI-PRP: désigne le cumul de l'évaluation des facteurs relatifs à la vie privée et de l'analyse de sécurité produites pour un projet d'acquisition, de refonte ou de mise à jour d'un système d'information.

Communauté universitaire : désigne toute personne, qui notamment :

- exerce une fonction, occupe un emploi rémunéré ou accomplit des tâches bénévolement à l'Université;
- poursuit des activités à titre de stagiaire (incluant un stage postdoctoral);
- fait partie d'une association ou d'un groupe relié à l'Université;
- a des relations avec l'Université à titre de personne cliente, visiteuse, personne invitée, personne ayant des contrats de services ou d'approvisionnement avec l'Université, personne sous-traitante ou locataire.

Évaluation des facteurs relatifs à la vie privée (EFVP): désigne la démarche préventive obligatoire qui vise à mieux protéger les renseignements personnels et à respecter davantage la vie privée des personnes physiques.

Intelligence artificielle : ensemble des théories et des techniques développant des programmes informatiques complexes capables de simuler certains traits de l'intelligence humaine tels que le raisonnement, l'apprentissage et l'entraînement.

- L'intelligence artificielle dite générative est un type d'intelligence artificielle qui génère du contenu en modélisant les caractéristiques des données qui alimentent un modèle. Elle peut créer du nouveau contenu sous plusieurs formes, comme du texte, une image, un fichier audio ou vidéo ainsi que du code logiciel.
- L'intelligence artificielle dite agentique est un système conçu pour interagir avec les données et les outils d'une manière qui nécessite une intervention humaine minimale. Ces systèmes ont la capacité de prendre des décisions de manière autonome en fonction des données et outils qui l'alimentent.

Outil d'IA public : outil d'intelligence artificielle offert en accès public, notamment sur un navigateur Web.

Personnel cadre : toute personne embauchée pour occuper un poste de cadre à l'Université.

Renseignement personnel : désigne les renseignements qui portent sur une personne physique et permettent de l'identifier. Ils sont confidentiels. Le nom d'une personne physique n'est pas un renseignement personnel, sauf lorsqu'il est mentionné avec un autre renseignement concernant cette personne ou lorsque sa seule mention révélerait un renseignement personnel la concernant.

Sont notamment du domaine public et ne sont pas personnels les renseignements suivants :

- nom, titre, fonction, classification, traitement, l'adresse et le numéro de téléphone professionnels d'un membre du personnel d'un organisme public;
- un renseignement concernant une personne en sa qualité de partie à un contrat de service conclu avec un organisme public.

Renseignement personnel sensible : désigne un renseignement personnel qui, notamment par sa nature médicale, biométrique ou autrement intime ou en raison du contexte de son utilisation ou de sa communication, suscite un haut degré d'attente raisonnable en matière de respect de la vie privée.

Unité administrative : regroupement de personnes qui exercent des activités dont la gestion est sous la responsabilité du personnel cadre.

6 RÔLES ET RESPONSABILITÉS

6.1 Secrétariat général

- a) Le Secrétariat général est responsable de la diffusion de la présente politique au sein de la communauté universitaire.
- b) L'équipe chargée de la protection des renseignements personnels de l'Université, relevant du Secrétariat général, veille à appliquer le cadre légal aux projets institutionnels impliquant l'IA et peut, à cet effet, demander des modifications au projet ou ne pas l'approuver en cas de non-conformité.

6.2 Personnel cadre

Le personnel cadre s'assure de diffuser et de faire appliquer les lignes directrices de la présente politique par les membres de son unité administrative.

6.3 Personnes utilisatrices

Les personnes utilisatrices d'un outil d'IA doivent, en tout temps, respecter les lignes directrices énoncées à la présente politique.

6.4 Comité sur la sécurité de l'information et le Comité sur l'accès à l'information et sur la protection des renseignements personnels (CSI-CAIPRP)

- a) Le CSI-CAIPRP, dans le cadre du mandat de chaque comité, est désigné, comme l'instance responsable du traitement et du suivi des dossiers d'IA à l'Université.
- b) Notamment, cette instance :
 - approuve les projets d'utilisation de l'IA lorsqu'ils lui sont soumis;
 - approuve la liste d'outils d'IA publics pouvant être utilisés par la communauté universitaire;
 - formule des recommandations quant à l'utilisation de l'IA à l'Université;
 - reçoit et, le cas échéant, collabore aux analyses SI-PRP concernant les outils IA.

6.5 Comités de réflexion

L'Université, dans la mise en œuvre de sa structure de gouvernance en matière d'IA, forme divers comités de réflexion chargés de partager les besoins, les opportunités, les enjeux et les préoccupations en lien avec l'utilisation de l'IA dans leur secteur d'activité, soit l'administration, l'enseignement et la recherche.

6.6 Comité conseil-IA

- a) L'Université, dans la mise en œuvre de sa structure de gouvernance en matière d'IA, forme un Comité conseil-IA chargé d'analyser les besoins, les opportunités et les enjeux en lien avec l'usage des outils d'intelligence artificielle à l'Université au niveau des pratiques administratives, des études, de l'enseignement et de la recherche, et fait des recommandations au CSI-CAIPRP.
- b) Ce Comité est formé, notamment, de personnes membres de l'équipe du Secrétariat général, du Service des technologies de l'information, du Décanat de la recherche et du Centre d'apprentissage, réussite et pédagogie universitaire.

7 LIGNES DIRECTRICES

7.1 Respecter la vie privée

Toute utilisation de l'IA doit respecter la confidentialité et la vie privée, en conformité avec la *Loi sur l'accès aux documents d'un organisme public et sur la protection des renseignements personnels*. À cet effet, la personne utilisatrice doit s'assurer de ne jamais inclure de renseignements personnels dans la formulation d'une requête.

7.2 Respecter la confidentialité

Toute utilisation de l'IA doit respecter la confidentialité de l'information détenue par l'Université. Ainsi, aucune information confidentielle de nature administrative, financière, stratégique ou politique, notamment, ne doit être incluse dans la formulation d'une requête.

7.3 Respecter les principes de droits d'auteur

- a) Toute utilisation de l'IA doit respecter les principes de droits d'auteur, dont la propriété intellectuelle.
- b) Ainsi, toute personne utilisatrice, au moment de formuler une requête, doit :
 - s'assurer de détenir les droits et autorisations requis sur le matériel ou les données nécessaires à la formulation de la requête;
 - s'abstenir d'inclure du matériel protégé par le droit d'auteur dans une requête sans s'être assuré, au préalable, que les termes d'une licence permettent cette utilisation ou qu'une exception légale peut s'appliquer dans de telles circonstances.

7.4 Assurer la sécurité de l'information

- a) Un outil d'IA est considéré comme un système d'information de l'Université lorsque celui-ci est déployé dans son infrastructure numérique. Lorsqu'il est nécessaire de faire l'acquisition d'un outil d'intelligence artificielle, celui-ci doit, au préalable, faire l'objet d'une analyse SI-PRP dont les conclusions seront favorables.
- b) Dans le cas de l'acquisition d'un outil d'intelligence artificielle, une analyse SI-PRP tiendra compte de plusieurs critères, notamment :
 - l'acceptabilité du risque au niveau de la cybersécurité;
 - l'offre d'une version payante ou d'une version offerte gratuitement au public;
 - la provenance de l'outil et le lieu d'hébergement des données;
 - l'utilisation projetée des données sensibles de l'organisation aux fins d'entraînement.

- l'élaboration d'un plan d'amélioration continue et de vérification de la fiabilité de l'outil d'IA analysé comprenant notamment des vérifications périodiques de la performance, des revues des pratiques et des tests de validation du comportement.

7.5 Agir de façon responsable

- a) L'utilisation de l'IA doit être faite de façon responsable. Il est de la responsabilité de la personne utilisatrice de mettre en œuvre, dans le cadre de ses fonctions, les bonnes pratiques d'utilisation afin de réduire les risques relatifs à l'utilisation de l'IA.
- b) Plus précisément, elle :
 - est responsable de s'assurer que l'utilisation de l'IA, incluant le contenu ajouté à toute requête, respecte le cadre légal et normatif de la vie privée, la confidentialité, la sécurité de l'information et les principes de droits d'auteur;
 - est responsable de s'assurer de l'intégrité et de la validité du contenu généré par une requête.

7.6 Décisions fondées sur un processus automatisé

- a) La *Loi sur l'accès aux documents d'un organisme public et sur la protection des renseignements personnels* encadre le recours à l'IA pour toute décision fondée sur un processus automatisé, c'est-à-dire tout processus où l'Université a recours à un système d'information afin de prendre une décision qui aura un impact sur une personne, individuellement.
- b) Le processus sera considéré comme automatisé lorsque l'outil ou le système d'information analyse l'information qui lui a été soumise et prend une décision individualisée sans l'intervention d'une personne physique, par exemple :
 - un système prend une décision sur l'admissibilité d'une personne à un programme, une bourse ou autre à partir des documents soumis par cette dernière;
 - un système prend une décision sur une demande de reconnaissance d'acquis à partir des documents soumis par une personne;
 - un système effectue la correction de travaux et octroie une note sans le regard d'une personne physique;
 - un système approuve ou refuse les demandes de congé ou de remboursements à la réception des pièces justificatives de la part d'une personne employée sans validation d'une personne physique.
- c) Le recours à l'IA pour les décisions fondées sur un processus automatisé doit être transparent et toute personne visée par une décision automatisée doit être en mesure d'y consentir ou de demander la révision de la décision auprès du service chargé de l'application de ce processus. Avant de mettre en place de tels processus, le Secrétariat général doit être informé afin de valider le respect des prérequis légaux de la démarche.

7.7 Autres considérations

En plus du respect des lignes directrices présentées aux sections 7.1 à 7.6, la personne utilisatrice doit :

- a) s'assurer que les résultats d'une requête ne contiennent pas de contenu biaisé, discriminatoire, non inclusif ou diffamatoire, dans le respect de la *Politique institutionnelle sur l'équité, la diversité et l'inclusion* (C3-D77);

- b) s'assurer de respecter les conditions d'utilisation de l'outil d'IA, notamment en évitant d'utiliser l'IA générative pour des activités suspectes, malicieuses ou malveillantes;
- c) en cohérence avec la *Politique environnementale de* (C3-D95), utiliser l'IA de manière à favoriser des comportements de l'ordre de la sobriété numérique. On entend par sobriété numérique toute démarche qui vise un usage avisé et modeste des technologies numériques dans l'objectif d'en réduire l'impact environnemental;
- d) être à l'affut des formations offertes par l'Université ou toute autre formation pertinente en IA.

7.8 Directives et indications d'application gouvernementales

Les directives et indications d'application émises par les autorités gouvernementales sont susceptibles de prévoir, à tout moment, des règles et des obligations applicables à l'utilisation de l'intelligence artificielle pouvant différer de celles contenues à la présente politique. En cas d'opposition entre celles-ci, celles prévues aux directives et indications d'applications gouvernementales auront préséance.

8 RESPONSABLE DE L'APPLICATION

Le Secrétariat général est responsable de l'application de cette politique.

9 MISE À JOUR

La présente politique est mise à jour tous les trois (3) ans, ou plus souvent si des modifications sont nécessaires.

10 ENTRÉE EN VIGUEUR

La présente politique entre en vigueur à compter de la date de son adoption par le Conseil d'administration.