
DIRECTIVE SUR L'UTILISATION DE L'INTELLIGENCE ARTIFICIELLE GÉNÉRATIVE

Numéro de directive : DINC-R1 DIR
Date d'entrée en vigueur : 1er juillet 2026

Pour tout le personnel

Portée : Tous les services et les unités administratives — personnel d'encadrement, enseignant, de soutien et professionnel.

Références normatives : Loi 25; directives et FAQ du MCN (IA-RI-2025-001-OP; IA-SI-2025-001-OP DeepSeek); Guide des bonnes pratiques (MCN, 2024); Cadre de référence et Guide pratique du MES (2025).

Énoncé de principes pour une utilisation responsable de l'IA (MCN, Arrêté 2025-02, 3 décembre 2025).

1. Objet et champ d'application

La présente directive encadre l'utilisation de l'intelligence artificielle générative (IAG) par le personnel du Cégep de l'Outaouais et précise ainsi les modalités d'application du règlement relatif à l'utilisation du Parc informatique et multimédia par le personnel DRIM-R1, en ce qui concerne l'utilisation de l'IAG. Elle est conforme aux exigences du ministère de la Cybersécurité et du Numérique (MCN) et s'inscrit dans le cadre des livrables attendus tel que défini dans le Portail IAG du MCN. Elle vise également à prévenir les risques en matière de protection des renseignements personnels, de sécurité de l'information et d'éthique, et à soutenir des usages responsables et transparents de l'IAG.

2. Définitions

- Assistant virtuel/IAG : application ou service qui génère des contenus (texte, image, code, etc.) à partir d'invites en langage naturel et qui peut interagir avec l'utilisateur.
- Donnée sensible : renseignements personnels, stratégiques, financiers, médicaux, dossiers RH, secrets commerciaux ou toute information protégée par la loi.
- Outil approuvé : solution IAG autorisée par l'institution et conforme aux exigences du MCN et du MES.
- EFVP (Évaluation des facteurs relatifs à la vie privée) : analyse exigée par la Loi 25 pour tout projet impliquant des renseignements personnels.

3. Principes directeurs

- 3.1 Conformité légale (Loi 25) et réglementaire (MCN/MES).
- 3.2 Protection des renseignements personnels : réduction de leur utilisation, confidentialité par défaut, journalisation et traçabilité.
- 3.3 Sécurité de l'information : contrôle d'accès, chiffrement, gestion des incidents.
- 3.4 Transparence et responsabilité : mention de l'usage d'IAG lorsque l'outil a contribué à un document officiel; vérification et approbation humaines.
- 3.5 Primauté du français dans les communications officielles et respect de l'accessibilité numérique; règles pour l'accessibilité des contenus Web (W3C) .

4. Interdictions et suspensions applicables

- 4.1 Suspension des assistants virtuels IAG non approuvés (IA-RI-2025-001-OP) : toute expérimentation, acquisition de licences ou intégration d'assistants virtuels IAG est suspendue jusqu'à nouvel ordre, sauf exceptions autorisées.
- 4.2 Interdiction d'utiliser DeepSeek (IA-SI-2025-001-OP) : l'utilisation de tout assistant virtuel DeepSeek (applications, sites, code source) est interdite. Selon les directives du MCN ou des différents cadres légaux, la liste d'interdiction pourrait changer.
- 4.3 Interdiction d'entrer des renseignements personnels, confidentiels ou stratégiques dans des outils IAG publics ou non approuvés.
- 4.4 Interdiction de décisions administratives ou disciplinaires entièrement automatisées; une validation humaine est obligatoire pour toute décision affectant des droits ou des services.

5. Exemples d'usages permis (avec contrôle)

Sous réserve des articles 4 et 8 et lorsque des outils approuvés sont disponibles :

- 5.1 Personnel administratif et enseignant : génération de brouillons, de synthèses non sensibles, de reformulations; traduction de documents non sensibles; production de modèles de lettres; création de contenu pédagogique; structuration de courriels; recherche d'informations publiques; planification et comptes rendus internes.
- 5.2 Cadres : production de synthèse documentaire; génération de scénarios et d'analyses non sensibles; traduction de documents non sensibles; veille réglementaire; préparation de notes stratégiques; optimisation de processus.
- 5.3 Toutes les productions assistées par IAG doivent faire l'objet d'une revue humaine et, au besoin, comporter une mention de contribution de l'IAG.



5.4 Inclusion et équité : mettre en place des mesures pour éviter la fracture numérique et promouvoir la diversité et l'inclusion : accessibilité universelle (WCAG), conception inclusive, implication de personnes représentatives des clientèles visées, accompagnement du personnel lorsque les métiers sont transformés par l'IA.

5.5 Explicabilité renforcée : tout système d'IA influençant des décisions, des prédictions ou des actions concernant des citoyens ou des entreprises doit fournir des explications claires et sans ambiguïté. Des mécanismes d'explicabilité (journalisation, critères, documentation) sont exigés; lorsque possible, recourir à des modèles ouverts pour faciliter la compréhension, la reproductibilité et l'explicabilité.

5.6 Modèles spécialisés : lorsque le besoin et les données sont spécifiques à un domaine et qu'un niveau de précision élevé est requis, privilégier des modèles d'IA générative spécialisés (ou verticaux) lorsqu'ils sont disponibles et abordables.

6. Rôles et responsabilités

- Responsable de la protection des renseignements personnels (RPRP) : supervise la conformité avec la Loi 25, approuve les EFVP et le registre des incidents.
- DSI – DINC /DPI : autorise et suggère les outils IAG selon les directives du MCN, met en place les contrôles techniques (SSO, DLP, journalisation), assure la sécurité et la gestion des risques.
- DRHDO : encadrent l'usage en contexte de gestion du personnel, interdisent l'évaluation automatisée des performances et la sélection automatisée des candidatures.
- Utilisateurs : respectent la directive, suivent la formation obligatoire et signalent tout incident.

7. Gouvernance, évaluation et registre

7.1 Autorisation préalable : tout nouveau type d'usage d'IAG doit être documenté et soumis à l'approbation conjointe DRHDO/DINC.

7.2 EFVP obligatoire : pour tout projet impliquant des renseignements personnels ou intégrant l'IAG à un système institutionnel.

7.3 Registre des usages : tenir un registre des outils, des cas d'usage, des incidents, des sources, des versions et des décisions; effectuer une révision trimestrielle.

7.4 Qualité et vérification : validation humaine, vérification des faits et traçabilité des sources avant diffusion externe.

7.5 Durabilité : intégrer une évaluation des impacts environnementaux et des pratiques de sobriété numérique (optimisation de calcul, modèles/matériels éco-efficients, rationalisation des flux de données) dans les projets IA; refléter ces éléments dans les choix technologiques.

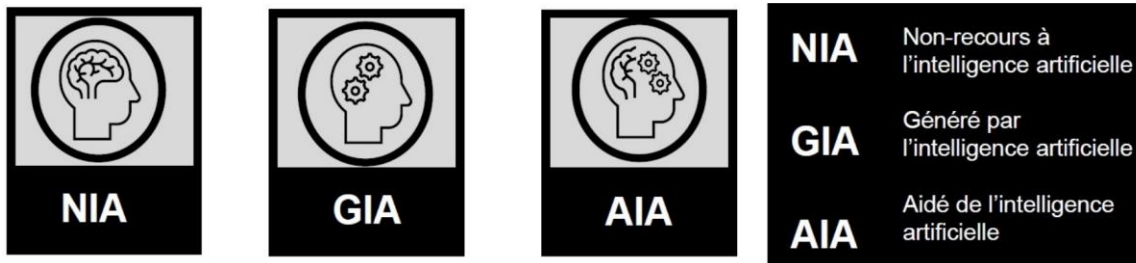
8. Gestion des données et sécurité

- 8.1 Réduction de l'utilisation et classification des données; anonymisation/pseudonymisation lorsque possible.
- 8.2 Interdiction de coller des données sensibles dans une requête; retrait les métadonnées avant tout traitement.
- 8.3 Hébergement et localisation conformes aux exigences gouvernementales; accès restreint et journalisation.
- 8.4 Procédure de signalement d'incident : avis au RPRP et DSI-DINC; mesures d'atténuation; consignation au registre; notification à la CAI lorsque requis.

9. Communication et transparence

Adopter un visuel institutionnel informant clairement les citoyens et les entreprises lorsqu'un système d'IA est utilisé dans un service numérique ou une communication officielle.

- 9.1 Mention « assisté par IA » lorsque l'apport de l'outil influence un document officiel ou une recommandation.
- 9.2 Interdiction de citer l'IAG comme source; seules des sources vérifiables doivent être citées.
- 9.3 Respect du français et du ton institutionnel; contrôle de qualité renforcée pour les communications externes.



10. Formation et soutien

- 10.1 Formation annuelle obligatoire pour l'ensemble du personnel ((Loi 25, sécurité, bonnes pratiques IAG). Le développement de cette technologie étant plus rapide que son encadrement, des formations régulières sont pertinentes.
 - 10.2 Guides d'usage et capsules : rédaction assistée, gestion des données, gouvernance et éthique.
 - 10.3 Point de contact : unité de cybersécurité/DSI-DINC pour soutien et questions.
- La formation (incluant les contenus du MCN) est requise ****avant**** le déploiement et l'utilisation des systèmes autorisés; mise à jour des connaissances lorsque nécessaire.

11. Acquisition et déploiement d'outils IAG

11.1 Aucun abonnement à des assistants virtuels IAG ou aucune acquisition de ceux-ci sans autorisation formelle.

11.2 Clauses contractuelles : confidentialité, localisation des données, audits, droits de sortie, conformité Loi 25 et MCN.

11.3 Tests d'acceptation et plan de sortie avant tout déploiement approuvé.

11.4 Souveraineté numérique : Privilégier, lorsque possible, les fournisseurs québécois/canadiens et l'hébergement des données au Québec/Canada. Pour les données sensibles, prioriser le traitement et l'hébergement dans des centres sous contrôle de l'État; à défaut, documenter et justifier.

11.5 L'usage est fait à des fins de recherche et de développement

Toute exception doit être documentée, autorisée par le DSI-DRI et le RPRP et consignée au registre (consulter addenda de la recherche, annexe C).

12. Utilisation éclairé et responsable

L'établissement favorise une utilisation éclairée et responsable de l'IAG fondée sur le développement du jugement critique, le maintien de l'autonomie intellectuelle, la protection des renseignements, la transparence des usages, la préservation des relations humaines, l'équité, la durabilité et la responsabilité individuelle. L'IAG doit agir comme un outil de soutien aux apprentissages, au travail et à la prise de décision, sans se substituer à la réflexion, au discernement et à la responsabilité des personnes. Une attention particulière doit être portée aux risques de dépendance technologique et de délestage cognitif excessif.

L'établissement reconnaît également que les systèmes d'IAG reposent sur une consommation importante de ressources énergétiques et matérielles. En cohérence avec ses engagements en matière de développement durable, il privilégie une intégration réfléchie de ces technologies, fondée sur les principes de nécessité, de valeur ajoutée pédagogique ou d'efficacité, de transparence et de sobriété numérique.

13. Entrée en vigueur et révision

La directive entre en vigueur à la date indiquée et sera révisée au moins annuellement ou à la suite d'une mise à jour du MCN/MES ou de la Loi 25. Les unités doivent adapter leurs procédures internes dans les 60 jours suivant la publication.

Annexe A

Références normatives et documentaires

- MCN — Indication d'application IA-RI-2025-001-OP : suspension des assistants virtuels IAG.
- MCN — Indication d'application IA-SI-2025-001-OP : interdictions d'utilisation des assistants virtuels DeepSeek.
- MCN — Guide des bonnes pratiques d'utilisation de l'IAG (octobre 2024)
- MES — Cadre de référence et Guide pratique (août 2025).
- Loi 25 — Loi modernisant des dispositions législatives en matière de protection des enseignements personnels (entrées en vigueur 2022–2024)
- CyberQuebec.org cadre normatif Cybersécuritaire / LOI 25
- DRIM — DRIM-R1 Règlement relatif à l'utilisation du parc informatique et multimédia par le personnel.

Annexe B :

Liste complète des acronymes utilisés dans la directive

CAI : Commission d'accès à l'information

→ Doit être avisée de toutes fautes liées à l'application de la loi 25.

DG : Direction générale

→ Supervise la mise en œuvre de la directive et approuve les orientations stratégiques.

DPI : Dirigeant principal de l'information

→ Responsable de la gouvernance de l'information, de la conformité réglementaire et de la coordination des projets numériques.

DRHDO : Direction des ressources humaines et du développement organisationnel

→ Autorisation de tout nouveau cas d'usage de l'IA.

→ Encadre l'usage de l'IA dans la gestion du personnel et interdit les évaluations automatisées.

DSI-DINC: Direction des systèmes d'information - Direction de l'innovation numérique et de la cybersécurité

→ Gère les infrastructures technologiques, la sécurité et l'autorisation des outils d'IA générative.

RPRP : Responsable de la protection des renseignements personnels

→ Assure la conformité à la Loi 25, approuve les EFVP et gère le registre des incidents.

EFVP : Évaluation des facteurs relatifs à la vie privée

→ Analyse obligatoire (Loi 25) pour tout projet impliquant des renseignements personnels.

MCN : Ministère de la Cybersécurité et du Numérique

→ Émet les directives gouvernementales sur la sécurité et l'usage de l'IA.

MES : Ministère de l'Enseignement supérieur

→ Encadre les pratiques IA dans le réseau collégial et universitaire.

SSO : Single Sign-On

→ Authentification unique permettant d'accéder à plusieurs services avec une seule connexion.

DLP : Data Loss Prevention

→ Technologies et politiques visant à prévenir la fuite ou la divulgation de données sensibles.

WCAG : Web Content Accessibility Guidelines

→ Normes internationales pour rendre les contenus web accessibles aux personnes ayant des limitations fonctionnelles.

Annexe C :

ADDENDA : Volet – RECHERCHE

Utilisation de l'IA générative en contexte de recherche

ADDENDA À LA DIRECTIVE INSTITUTIONNELLE

Portée : Chercheur(-euse)s, enseignant(e)s-chercheurs(-euse)s, assistant(e)s de recherche et toute personne impliquée dans des projets scientifiques ou expérimentaux au sein de l'établissement.

1. Objet

Cet addendum précise les règles applicables à l'utilisation de l'IA générative (IAG) dans les activités de recherche, afin de concilier innovation, conformité légale (Loi 25), éthique et intégrité scientifique.

2. Principes spécifiques

- L'usage de l'IAG est autorisé pour la recherche, sous réserve des balises suivantes :
 - **Intégrité scientifique :** les résultats générés par IAG doivent être validés par des méthodes reconnues et ne peuvent être publiés sans vérification humaine.
 - **Transparence :** toute utilisation d'IAG dans tout rapport, publication ou communication scientifique doit obligatoirement faire l'objet d'une mention.

3. Autorisation et gouvernance

- **Comité IA et recherche :** Création d'un comité (DSI-DINC, RPRP, SRDP, direction scientifique) pour évaluer les projets impliquant l'IAG.
- **Registre spécifique :** Chaque projet utilisant l'IAG doit être inscrit dans un registre dédié (objectifs, outils, données, impacts).
- **Une EFVP doit être obligatoire** si des données personnelles ou sensibles sont utilisées.

4. Usages permis

- Préparation de synthèses, analyses exploratoires, génération de code expérimental, simulation, traduction de documents non sensibles.
- Utilisation et développement de modèles ouverts ou spécialisés pour garantir la reproductibilité.
- Autorisation d'outils non approuvés **uniquement** dans le cadre d'une expérimentation validée par le comité IA et recherche.

5. Gestion des données

- Données sensibles : il est nécessaire d'anonymiser la collecte d'information sensible ou demander un consentement explicite.
- Hébergement : il est nécessaire de prioriser les infrastructures québécoises/canadiennes ou conformes aux normes gouvernementales.
- Interdiction de coller des données personnelles dans des outils publics.

6. Publication et communication

- La mention « IAG utilisée » doit être inscrite dans les articles, les rapports et les présentations.
- Interdiction de citer l'IAG comme source; seules des sources vérifiables sont acceptées.

7. Formation

- Une formation est obligatoire pour les chercheurs (-euses) : éthique de l'IA, biais, explicabilité, conformité Loi 25.

8. Dérogations

- Toute dérogation doit être approuvée par le comité IA et recherche et être consignée au registre.