



DIRECTIVE RELATIVE À LA GOUVERNANCE DE L'INTELLIGENCE ARTIFICIELLE GÉNÉRATIVE (IAG)

Directive numéro :

SG-PR-1-2026

Décision numéro :

DG-R-25-26-0591

Entrée en vigueur :

16 juin 2026

Dans ce document, le genre masculin est utilisé dans son sens neutre de façon à alléger le texte.

TABLE DES MATIÈRES

1. OBJET	4
2. CHAMP D'APPLICATION	4
3. ENCADREMENT LÉGAL.....	4
4. DÉFINITIONS.....	5
5. PRINCIPES	6
6. RÔLES ET RESPONSABILITÉS.....	6
6.1. Direction générale.....	6
6.2. Comité de gouvernance de l'IAG (CGIAG).....	6
6.3.. Comité sur l'accès à l'information et la protection des renseignements personnels (CAIPRP).....	6
6.4. Chef de la sécurité de l'information organisationnelle (CSIO).....	7
6.5. Service des technologies de l'information (STI)	7
6.6. Gestionnaires	7
6.7. Personnel enseignant	7
6.8. Utilisateurs (membres du personnel, élèves, parents et tout autre utilisateur)	7
6.9. Partenaires externes et fournisseurs	8
7. PROCESSUS D'ÉVALUATION D'UN SYSTÈME D'IAG	8
7.1. Priorisation des cas d'usage.....	8
7.2. Gestion des risques.....	8
7.3. Registre des systèmes d'IAG et des cas d'usage	9
7.4. Mesures liées au cycle de vie d'un système d'IAG	9
8. USAGES INTERDITS.....	11

1. OBJET

La *Directive relative à la gouvernance de l'intelligence artificielle générative* (Directive) établit les règles, rôles et contrôles encadrant l'identification, l'expérimentation, l'acquisition, l'utilisation et le déclassement des systèmes d'intelligence artificielle générative (IAG) au sein du Centre de services scolaire de la Région-de-Sherbrooke (CSSRS), en conformité avec les exigences légales et gouvernementales applicables. Elle vise à :

- Assurer un usage responsable, transparent et sécuritaire de l'IAG dans l'administration publique;
- Protéger les renseignements personnels et l'information gouvernementale;
- Garantir la conformité aux lois, politiques et indications d'application gouvernementales;
- Favoriser des bénéfices mesurables pour la population, en soutenant les services publics et la reddition de comptes.

2. CHAMP D'APPLICATION

La Directive s'applique :

- à toutes les personnes en lien avec le CSS :
 - Les membres du personnel;
 - Les élèves inscrits dans les établissements du CSS et leurs parents;
 - Les consultants, stagiaires et tout tiers travaillant pour ou avec le CSS et ayant accès aux environnements numériques ou aux données de l'organisation;
 - Les partenaires externes et fournisseurs.
- à tout système d'IAG (interne, infonuagique, tiers, code, API, connecteurs) utilisé dans le cadre des fonctions du CSS;
- à toutes les données détenues par le CSS et aux données numériques gouvernementales.

3. ENCADREMENT LÉGAL

La Directive prend assise notamment sur les encadrements suivants :

- [Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement](#) (LGRI) – gouvernance des ressources informationnelles, sécurité de l'information, mobilité/valorisation des données numériques gouvernementales;

- [Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels](#) (LAI, aussi connue comme la Loi 25) – obligations de gouvernance, évaluations des facteurs relatifs à la vie privée (ÉFVP), incidents de confidentialité, transparence, consentement;
- Ministère de la Cybersécurité et du Numérique du Québec (MCN) – [Indication d'application](#) (19 décembre 2025) et [Énoncé de principes pour une utilisation responsable de l'intelligence artificielle par les organismes publics](#) (gouvernance, gestion des risques, formation, critères de sélection des cas d'usage);
- Secrétariat du Conseil du trésor (SCT) – [Stratégie d'intégration de l'intelligence artificielle dans l'administration publique 2021 2026](#) (SCT).

4. DÉFINITIONS

Intelligence artificielle (IA)	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 influencer sur des environnements physiques ou virtuels. Différents systèmes d'IA présentent des degrés variables d'autonomie et d'adaptabilité après déploiement.
Intelligence artificielle générative (IAG)	Ensemble des techniques d'intelligence artificielle utilisées pour produire du contenu au moyen d'algorithmes et de mégadonnées, généralement sous forme de fichier texte, son, vidéo ou image.
Cas d'usage	Description des exigences comportementales d'un système et de son interaction avec un utilisateur. Un cas d'usage décrit l'objectif des utilisateurs ainsi que les exigences, y compris la séquence d'interactions entre les utilisateurs et le système.
Renseignements personnels (RP)	Toute information concernant une personne physique et permettant de l'identifier directement ou indirectement (ex. : nom, adresse, courriel personnel, date de naissance, dossier scolaire, informations médicales).
Données numériques gouvernementales (DNG)	Actifs informationnels stratégiques régis par le MCN et la LGRI (mobilité, qualité, sécurité, sources officielles).
Évaluation des facteurs relatifs à la vie privée (ÉFVP)	Analyse obligatoire dans les situations prévues par la LAI (ex. : acquisition/développement d'un système impliquant des renseignements personnels). La Commission d'accès à l'information a produit un <u>Guide d'accompagnement à l'évaluation des facteurs relatifs à la vie privée</u> et un <u>modèle générique de rapport d'ÉFVP</u> à utiliser pour effectuer cette analyse.
Incident de confidentialité	Accès, utilisation ou communication non autorisé d'un renseignement personnel, perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.

5. PRINCIPES

Les douze (12) principes exposés dans l'Énoncé de principes pour une utilisation responsable de l'intelligence artificielle par les organismes publics (MCN) s'appliquent à l'utilisation des systèmes d'IAG par le CSS et par les personnes visées par la Directive.

6. RÔLES ET RESPONSABILITÉS

L'application efficace de la présente Directive repose sur la compréhension et le respect des rôles et responsabilités qui suivent :

6.1. Direction générale

- Adopter la présente Directive et en assurer la revue périodique pour garantir sa pertinence face à l'évolution rapide de l'IA.
- Allouer les ressources nécessaires (humaines, technologiques et financières), notamment pour la formation et la sécurisation des infrastructures.

6.2. Comité de gouvernance de l'IAG (CGIAG)

- Autoriser les cas d'usage des systèmes d'IAG en s'assurant d'un retour sur investissement, de l'obtention de bénéfices et d'une gestion des risques adéquate.
- Effectuer le suivi des risques, approuver les plans de mitigation, décider des arrêts et relances, notamment en cas de suspension gouvernementale.
- Élaborer et mettre en œuvre un programme de formation et de sensibilisation incluant minimalement les formations proposées par le MCN (risques liés à l'utilisation de l'IAG, usage responsable, etc.).
- Rendre disponible un guide interne prévoyant les cas d'usage autorisés et ceux qui sont interdits ou soumis à des restrictions.
- Tenir à jour le Registre des systèmes d'IAG et des cas d'usage prévu au paragraphe 7.2 de la Directive.
- Suivre les développements technologiques et proposer des orientations stratégiques à la direction générale.

Le Comité de gouvernance de l'IAG (CGIAG) est composé des membres du CAIPRP, présenté au point 6.3, auxquels s'ajoutent le CSIO et la direction du Service des technologies de l'information (STI).

6.3. Comité sur l'accès à l'information et la protection des renseignements personnels (CAIPRP)

- Veiller à l'application de la LAI (règles de gouvernance, EFVP, incidents de confidentialité, consentements) et à la tenue des registres requis.
- Évaluer le niveau de risque résiduel d'atteinte à la vie privée d'un système d'IAG.
- Analyser, prioriser et soumettre des recommandations sur les cas d'usage au comité de gouvernance de l'IAG.

6.4. Chef de la sécurité de l'information organisationnelle (CSIO)

- Appliquer la LGGRI et les indications d'application du MCN (contrôles techniques, classification, journalisation, restrictions d'outils).

6.5. Service des technologies de l'information (STI)

- Évaluer les systèmes d'IAG, notamment quant aux normes de sécurité.
- Mettre en place des mesures de cybersécurité pour protéger l'infrastructure contre les menaces spécifiques à l'IAG.
- Soutenir le personnel dans l'intégration technique des outils d'IAG approuvés et en assurer la maintenance.

6.6. Gestionnaires

- Mettre en œuvre la Directive et veiller à son application uniforme dans tous les établissements et services.
- Promouvoir une culture de citoyenneté numérique responsable et d'intégrité intellectuelle auprès du personnel et des élèves.

6.7. Personnel enseignant

- Intégrer l'IAG de manière pédagogiquement pertinente et critique dans les activités, conformément aux objectifs d'apprentissage.
- Définir clairement aux élèves les consignes d'utilisation de l'IAG dans le cadre des travaux et évaluations.
- Modéliser l'utilisation éthique et responsable de l'IAG et développer la pensée critique des élèves face aux contenus générés.
- Protéger les renseignements personnels et les données institutionnelles en s'abstenant de les insérer dans les outils d'IAG non approuvés.

6.8. Utilisateurs (membres du personnel, élèves, parents et tout autre utilisateur)

- Respecter la présente Directive.
- Utiliser uniquement les systèmes autorisés par le CSS.
- Ne pas divulguer d'information confidentielle dans des systèmes non autorisés et signaler tout incident de confidentialité, le cas échéant.

6.9. Partenaires externes et fournisseurs

- Garantir la conformité légale de leurs solutions d'IAG lorsqu'elles sont utilisées par le CSS.
- Fournir une transparence totale sur la manière dont les données du CSS sont traitées, utilisées et sécurisées par leurs systèmes d'IAG.
- Respecter les ententes contractuelles et les exigences de sécurité du CSS.

7. PROCESSUS D'ÉVALUATION D'UN SYSTÈME D'IAG

7.1. Priorisation des cas d'usage

Les cas d'usage des systèmes d'IAG sont pertinents si l'utilisation d'un tel système est essentielle à la résolution d'un problème réel, à l'amélioration d'un processus, à l'amélioration des services offerts à la population (efficacité, efficacité et pertinence) ou à d'autres bénéfices (impacts positifs, gains, réduction des coûts).

Chacun des cas d'usage doit être documenté, en précisant notamment :

- La description générale du système d'IAG qui sera utilisé;
- La description générale de l'utilisation prévue du système d'IAG;
- La justification de la pertinence de l'utilisation prévue d'un système d'IAG;
- Une évaluation des gains anticipés.

Les cas d'usage doivent être analysés et priorisés en considérant non seulement les bénéfices anticipés, mais également les risques encourus.

7.2. Gestion des risques

Toute utilisation d'un système d'IAG doit être basée sur une démarche de gestion des risques. Cette démarche doit être exhaustive; elle doit notamment comprendre les étapes qui suivent :

- Identifier tous les risques organisationnels encourus par l'utilisation d'un système d'IAG. Ces risques peuvent, sans s'y limiter, être observés dans les matières suivantes : éthique, sécurité de l'information, gouvernance de données, juridique;

- Analyser les risques et documenter leurs principales causes et conséquences;
- Évaluer les risques et, en fonction notamment des résultats, prioriser leur traitement;
- Déterminer des mesures de mitigation, les responsables de leur mise en œuvre ainsi que les échéances;
- Approuver les résultats;
- Effectuer le suivi et la revue des risques en fonction du processus organisationnel défini.

Dès la phase de conception d'un projet d'acquisition, de développement ou de refonte d'un système d'IAG, et lors de la définition des cas d'usage, le CSS doit procéder à une ÉFVP. Cette ÉFVP doit être actualisée tout au long des phases d'expérimentation, de développement et de déploiement du projet qui concerne un système d'IAG. Le cas échéant, le CAIPRP doit accepter le niveau de risque résiduel d'atteinte à la vie privée pour poursuivre les activités. Cette exigence vaut pour tous les systèmes d'IAG incluant ceux qui, à première vue, ne semblent pas impliquer de renseignements personnels. Dans le cas de ces derniers, le CSS doit procéder à l'ÉFVP laquelle pourra confirmer l'absence de renseignements personnels.

La démarche de gestion des risques, incluant l'ÉFVP, doit être révisée périodiquement en fonction de l'évolution du système d'IAG et de son contexte d'utilisation.

7.3. Registre des systèmes d'IAG et des cas d'usage

Le CSS tient un registre des systèmes d'IAG et des cas d'usage recensant les finalités, les données utilisées et leurs catégories (incluant présence de renseignements personnels), emplacements et accès, fournisseurs, mesures de sécurité, EFVP, décisions prises, responsables, périodes de révision et toute autre information pertinente.

7.4. Mesures liées au cycle de vie d'un système d'IAG

7.4.1. Planification et conception

- Évaluer les risques pour démontrer l'intérêt public, l'alignement stratégique et l'absence de solutions moins intrusives.

7.4.2. Collecte et traitement des données

- Déterminer si des renseignements personnels sont en jeu, déclencher l'EFVP et consulter le CAIPRP.
- Assurer la qualité et la conformité des données numériques utilisées dans un système d'IAG tout au long de leur cycle de vie (création, collecte,

conservation, utilisation, transmission, communication, archivage et destruction).

- Appliquer le [Modèle de classification de sécurité des données numériques gouvernementales approuvé par le MCN pour protéger les DNG utilisées](#).
- Interdire toute saisie de renseignements de nature confidentielle dans un système d'IAG public.¹

7.4.3. Construction du modèle ou adaptation d'un modèle existant

- Privilégier des environnements gouvernementaux ou contractualisés (infonuagique conforme).
- Assurer un contrôle strict des droits d'accès au système d'IAG.
- Respecter les consignes en vigueur, notamment quant aux suspensions ou limitations.
- Dans tout contrat avec un fournisseur, intégrer des clauses portant sur : résidence/lieu de traitement, usage secondaire, conservation/suppression, traçabilité, droits d'audit, gestion d'incidents, biais et performance.

7.4.4. Test, évaluation, vérification et validation

- Mettre en place des tests de performance (efficacité et qualité des résultats) pour vérifier la fiabilité et la robustesse du système d'IAG et apporter les ajustements requis avant le déploiement.
- Établir un processus d'amélioration continue pour chaque système d'IAG utilisé, le documenter et l'appliquer. Ce processus vise à s'assurer que le système d'IAG demeure efficace et conforme à une utilisation responsable.
- Développer un plan de supervision humaine adéquate et une journalisation des interactions.
- S'assurer que tout système d'IAG utilisé ayant un impact sur des décisions, des prédictions ou des actions concernant les citoyens ou les entreprises, intègre des mécanismes qui assurent des explications claires et sans ambiguïté. L'utilisation de modèles d'IAG ouverts², lorsque cela est possible, doit alors être privilégiée.

¹ Système d'IAG public : toute version « grand public » gratuite ou non de systèmes d'IAG, comme les versions en ligne de Copilot (incluant Copilot Chat) et de ChatGPT, pour autant qu'elle ne soit pas interdite par le CSS.

² Un modèle d'IAG ouvert est un modèle dont au moins certains des composants (code, paramètres finaux, documentation, etc.) sont rendus publiquement accessibles, et ce, dans un cadre de licences et d'informations qui permettent son usage, son étude, sa modification ou sa redistribution. Le degré d'ouverture peut varier.

7.4.5. Mise à disposition pour utilisation

- Élaborer et mettre en œuvre un programme de formation et de sensibilisation aux risques liés à l'utilisation du système d'IAG, incluant une mise à jour des connaissances lorsque nécessaire.
- Assurer une gestion du changement adaptée à l'impact organisationnel de l'introduction d'un système d'IAG et permettre l'introduction de cette technologie de manière optimale.

7.4.6. Exploitation et suivi

- Assurer une surveillance continue du système d'IAG, notamment par des mesures pour vérifier sa fiabilité, sa robustesse et son utilisation responsable.
- S'assurer de la mise à jour des mesures de sécurité applicables.
- Effectuer une revue périodique des modèles, des jeux de données, des dérives, des biais et des incidents.

7.4.7. Mise hors service

- Procéder à un arrêt de service si non-conformité, en cohérence avec les indications du MCN.
- Supprimer ou désactiver les accès au système d'IAG.
- Assurer la gestion des données du système d'IAG, notamment par leur archivage ou leur destruction conformément au calendrier de conservation du CSS.

8. USAGES INTERDITS

Sont interdites :

- La transmission de renseignements personnels ou d'information confidentielle³ ou sensible⁴ dans des systèmes d'IAG non autorisés;
- Les décisions entièrement automatisées produisant des effets juridiques ou similaires, sans intervention et validation humaines explicites;
- La génération ou diffusion de contenus trompeurs, discriminatoires, diffamatoires ou contraires aux lois et valeurs du service public.

Toute personne visée par la Directive qui constate un usage non conforme de l'IAG doit le signaler rapidement au Service des technologies de l'information du CSS.

³ Information confidentielle dont la divulgation, l'altération, la perte ou la destruction sont susceptibles de porter préjudice à la personne ou à l'organisation qu'elle concerne.

⁴ Information qui ne doit être communiquée ou rendue accessible qu'aux personnes et aux entités autorisées.