GUIDE D'APPLICATION DES MESURES APPLICABLES LORS DE L'UTILISATION DE L'INTELLIGENCE ARTIFICIELLE GÉNÉRATIVE

MINISTÈRE
DE LA CYBERSÉCURITÉ
ET DU NUMÉRIQUE

Votre gouvernement

Québec

RÉDACTION
La Direction de l'encadrement
et de l'utilisation éthique de l'intelligence artificielle
du Sous-ministériat adjoint au dirigeant principal de l'information et à
la gouvernance du ministère de la Cybersécurité et du Numérique

ÉDITION
La Direction des communications du ministère
de la Cybersécurité et du Numérique

Si vous éprouvez des difficultés techniques ou si vous souhaitez obtenir une version adaptée du document, veuillez communiquer avec la Direction des communications :

Direction des communications
Ministère de la Cybersécurité et du Numérique
900, place D'Youville, 2e étage
Québec (Québec) G1R 3P7
Courriel : information@mcn.gouv.qc.ca

TABLE DES MATIÈRES

ABRÉVIATIONS

AE	architecture d'entreprise
AIPRP	accès à l'information et protection des renseignements personnels
ARP	analyse des risques du produit
DNG	données numériques gouvernementales
ÉFVP	évaluation des facteurs relatifs à la vie privée
ÉFVP-R	évaluation des facteurs relatifs à la vie privée et des risques
FAQ	foire aux questions
GIR	gestion intégrée des risques
IA	intelligence artificielle
IAG	intelligence artificielle générative
LAI	*Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (chapitre A-2.1)
LCCJTI	*Loi concernant le cadre juridique des technologies de l'information* (chapitre C-1.1)
LGGRI	*Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (chapitre G-1.03)
LRSSS	*Loi sur les renseignements de santé et de services sociaux* (chapitre R-22.1)
MCN	ministère de la Cybersécurité et du Numérique
OP	organismes publics
PRP	protection des renseignements personnels
RH	ressources humaines
RLRQ	recueil des lois et des règlements du Québec
SI	sécurité de l'information

OBJECTIF DU GUIDE

Ce guide vise à fournir un cadre pratique pour la mise en œuvre des « Mesures applicables lors de l'utilisation de l'intelligence artificielle générative [1]». Il traduit ces mesures en actions concrètes.

Ces actions doivent être proportionnelles aux risques encourus et aux bénéfices recherchés par la mise en œuvre d'un système d'intelligence artificielle générative (IAG)[2] (Considération de la proportionnalité de l'*Énoncé de principes pour une utilisation responsable de l'intelligence artificielle par les organismes publics* [ci-après « l'Énoncé »][3]). Rappelons que cet énoncé présente les principes que les organismes publics (OP) assujettis à la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*[4] (LGGRI) doivent mettre en œuvre tout au long du cycle de vie des systèmes d'intelligence artificielle[5].

Le guide s'applique :

- à tous les projets, produits ou services intégrant des systèmes d'IAG;
- aux équipes de développement, de recherche, de gouvernance des données, de conformité et de gestion des risques;
- aux partenaires externes impliqués dans la conception, l'implémentation ou l'utilisation de systèmes d'IAG; en effet, l'OP doit s'assurer que les actions proposées dans ce guide sont respectées, notamment en garantissant que les clauses contractuelles reflètent ces actions.

---

[1] IA-RI-2025-003-OP.
[2] « 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 ». *Office québécois de la langue française.*
[3] Arrêté numéro 2025-02 du ministre de la Cybersécurité et du Numérique en date du 3 décembre 2025.
[4] RLRQ, c. G -1.03.
[5] Cycle de vie des systèmes d'IA :
phases d'un cycle de vie de tels systèmes, notamment 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, d'évaluation, de vérification et de validation, la phase de mise à disposition pour son utilisation, la phase d'exploitation et de suivi et la phase de mise hors service.

Ce guide ne couvre pas :

- les systèmes d'IA[6] non générative (ex. : systèmes de recommandation, IA prédictive, etc.);
- les aspects techniques détaillés de l'implémentation logicielle (couverts par des guides techniques spécifiques);
- les politiques organisationnelles générales sur l'IA.

[6] Système d'intelligence artificielle :
Le sens que donne le Conseil sur l'intelligence artificielle de l'Organisation de coopération et de développement économiques à « système d'intelligence artificielle ou système d'IA », et ses modifications subséquentes. Cette expression désigne actuellement 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. »

1. GOUVERNANCE ORGANISATIONNELLE POUR LES SYSTÈMES D'IAG

1.1. Instauration d'une structure de gouvernance adaptée au contexte de l'organisation

La structure de gouvernance mise en place par un OP pour garantir l'utilisation responsable des systèmes d'IAG doit répondre à la réalité de son organisation. La structure pour l'IAG s'inscrit dans la gouvernance de l'organisation. Le dirigeant de l'OP approuve le cadre de gouvernance et donc la nomination de la ou les personnes ayant l'autorité de permettre l'utilisation d'un système d'IAG. La structure de gouvernance pour les systèmes d'IAG doit être arrimée avec la structure de gouvernance des données numériques gouvernementales (DNG[7]). La mise en place d'une structure de gouvernance par l'OP devrait être conforme au principe de responsabilité de l'Énoncé de principes pour une utilisation responsable de l'IA. Ceci implique de définir, d'élaborer et d'appliquer les exigences et les mécanismes de contrôle appropriés, en fonction des cas d'usage identifiés et priorisés, pour tout système d'IAG qu'il prévoit concevoir, acquérir, expérimenter ou déployer.

Plus précisément, il est recommandé que la structure de gouvernance :

- implique les secteurs clés de l'OP jugés pertinents dans les comités ou les groupes de travail établis aux fins de coordination et de concertation en matière de systèmes d'IAG, notamment : sécurité de l'information (SI), juridique, accès à l'information et protection des renseignements personnels (AIPRP), éthique, ressources humaines (RH), experts de données, gestion des risques, architecture d'entreprise (AE), ressources financières;
- permette d'établir clairement l'unité responsable en :
    - identifiant les personnes ayant les rôles et responsabilités liés à la gouvernance des systèmes d'IAG, dont celui relatif à l'autorisation des cas d'usage, ou aux exceptions, le cas échéant;
    - faisant connaître les directives et processus en matière d'IAG auprès du personnel;
    - s'assurant du respect des directives et des processus en matière d'IAG.
- prévoie un cadre adapté au contexte organisationnel qui favorise le développement et le déploiement efficaces et responsables d'un système d'IAG;

[7] Sous réserve des exclusions prévues à l'alinéa 2 de l'article 12.10 de la LGGRI, on entend par DNG toute information portée par un support technologique détenue par un OP.

- définisse et permette d'appliquer un processus clair et documenté pour proposer et valider de nouveaux cas d'usage à valeur ajoutée pour l'OP :
    - définisse et permette d'appliquer un processus décisionnel pour permettre aux autorités de l'OP de prendre des décisions éclairées en tenant compte des risques organisationnels, éthiques, juridiques, et de sécurité liés aux systèmes d'IAG.

- élaborer et tenir à jour un processus décisionnel permettant au DI de faire des choix éclairés au regard de tous les risques liés aux systèmes d'IAG.

Exemple d'application — Mise en place d'une gouvernance pour l'utilisation d'un système d'IAG public

« Un OP souhaite permettre l'utilisation d'un système d'IAG public à usage général (ex. : un assistant conversationnel en ligne), mais souhaite encadrer cette utilisation pour garantir la sécurité et la conformité. »

Pour répondre à la mesure applicable 1.1 sur la gouvernance, l'OP met en place la structure de gouvernance pour les systèmes d'IAG s'appuyant sur la gouvernance des DNG déjà en place, tout en intégrant les spécificités liées à l'IA et en assurant la conformité aux exigences de sécurité, de protection des renseignements personnels et d'éthique. Le tableau suivant donne des exemples des actions attendues :

Obligation/Recommandation	Description/Action attendue
Créer une structure de gouvernance adaptée à l'organisation	Arrimée à la gouvernance des DNG
Impliquer les secteurs clés dans les comités ou groupes de travail	SI, juridique, AIPRP, éthique, RH, experts de données
Déterminer les usages autorisés du système d'IAG	Approuver les cas d'usage et exceptions
Faire connaître les directives et processus en matière d'IAG	Sensibilisation et communication

1.2. Gestion des risques liés à l'utilisation des systèmes d'IAG

Une gestion des risques doit être réalisée dès la conception et la mise à jour lors des phases **d'expérimentation, de développement, de déploiement** et lors des **acquisitions** des systèmes d'IAG. Elle s'applique à tous les systèmes d'IAG, même sans renseignement personnel. Avant le déploiement, le niveau de risque, en considérant les mesures de mitigation mises en œuvre, doit être acceptable pour la personne qui a l'autorité de permettre l'utilisation d'un système d'IAG.

La gestion des risques s'inscrit dans la gestion des risques organisationnels. Plus spécifiquement, pour les systèmes d'IAG, la démarche structurée suivante proposée par le MCN, appuyée par des outils (réf. : figure 1), inclut les étapes suivantes :

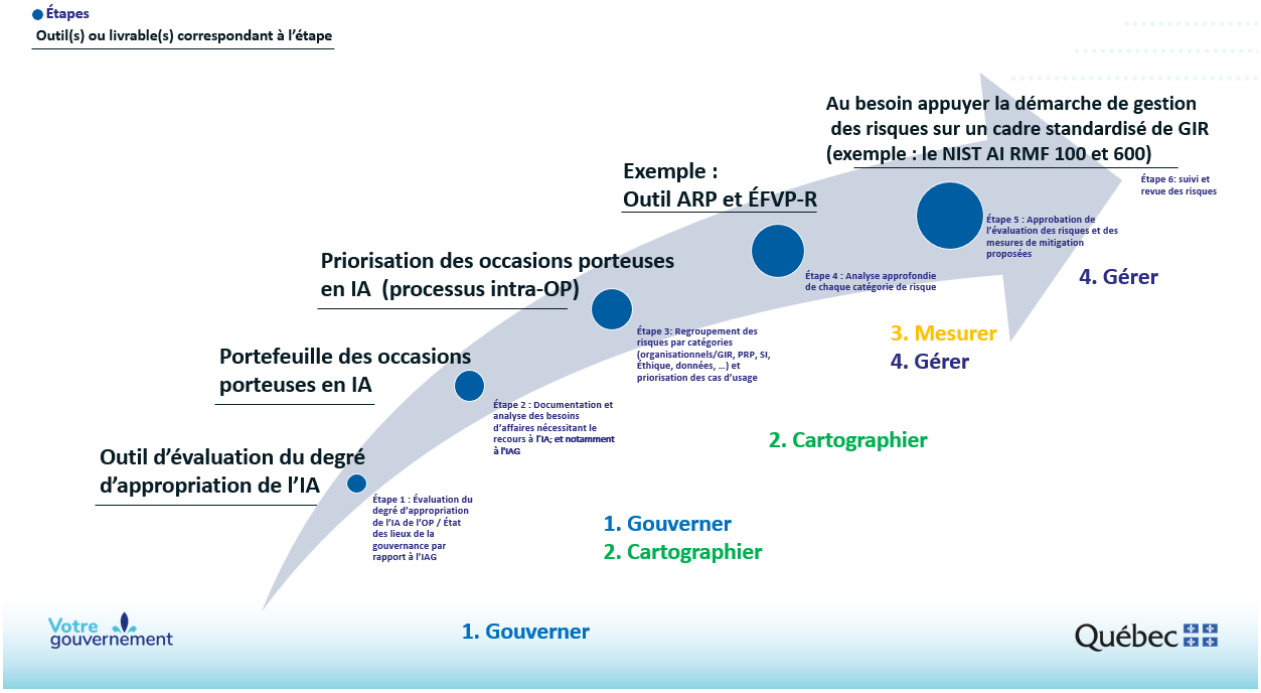

Figure 1 : Étapes de la démarche d'évaluation et de la gestion des risques liés à l'intégration et à l'utilisation d'un système d'IAG.

Note : l'analyse de risques ne se limite pas à l'ARP et à l'ÉFVP-R fournis par le MCN. Il revient à l'OP d'analyser tous les risques ou toutes les catégories de risques de manière détaillée.

1. Étape 1 : évaluation du degré d'appropriation de l'IA par l'OP
   Il est recommandé aux OP d'établir une évaluation de leur capacité organisationnelle à assurer une utilisation responsable des systèmes d'IAG. Pour faire une telle évaluation, l'OP peut s'appuyer sur **l'outil d'évaluation du degré d'appropriation de l'IA par l'OP** du MCN. Cette étape de la démarche permet de déterminer le niveau de maturité de l'OP pour la mise en œuvre de l'IA en identifiant les mesures et les éléments mis de l'avant par celui-ci dans les dimensions suivantes :

   a. Stratégie;
   b. Processus;
   c. Données;
   d. Technologie;
   e. Ressources humaines et culture organisationnelle;
   f. Éthique et gouvernance.

2. Étape 2 : documentation et analyse des besoins d'affaires
   La documentation et l'analyse des cas d'usage[8] peuvent s'appuyer sur le **gabarit du portefeuille des occasions porteuses en IA** proposé par le MCN**.** L'objectif de cette étape est de minimalement permettre la documentation et l'analyse des éléments suivants :
   a. La pertinence de l'utilisation prévue des systèmes d'IAG (principe de l'efficience, de l'efficacité et de la pertinence);
   b. Les données impliquées, notamment la nature, le niveau de sensibilité de celles-ci (principe du respect des personnes et de la règle de droit, principe de la fiabilité et de la robustesse).

3. Étape 3 : priorisation des occasions porteuses en IA en se basant sur les processus existants de priorisation de l'OP ou en utilisant le **gabarit du portefeuille des occasions porteuses en IA** en pondérant à partir notamment de la présence ou non des risques organisationnels, notamment :
   a. Les risques juridiques, notamment ceux d'atteinte à la vie privée, et réglementaires, notamment ceux associés à des obligations légales incompatibles avec les lois et les textes d'applications québécoises;
   b. Les risques liés à la sécurité de l'information;
   c. Les risques éthiques.

[8] Cas d'usage : Description des exigences comportementales d'un système et de son interaction avec un utilisateur [ISO, 2018]. Un cas d'utilisation décrit l'objectif des utilisateurs ainsi que les exigences, y compris la séquence d'interactions entre les utilisateurs et le système.

4. Étape 4 : analyse et évaluation approfondie de chaque catégorie de risque
   L'objectif de cette étape de la démarche est :
   a. de permettre à l'OP d'évaluer les risques et, en fonction notamment des résultats, de prioriser leur traitement;
   b. déterminer des mesures de mitigation;
   c. d'identifier d'emblée les responsables de l'application des mesures de mitigation et de planifier la mise en place de ces dernières. Pour les risques liés au produit, il est recommandé de s'appuyer sur **l'outil d'analyse des risques du produit (ARP**), puis d'approfondir les risques d'atteinte à la vie privée[9] des cas d'usage avec **l'outil d'évaluation des facteurs relatifs à la vie privée et des risques (ÉFVP-R)** [10] du MCN.

5. Étape 5 : approbation de l'analyse de risque
   L'autorité désignée au sein de l'OP devra prendre une décision à la vue de l'évaluation des risques et des mesures de mitigation proposées afin d'approuver l'utilisation du système d'IAG.

6. Étape 6 : effectuer le suivi et la revue des risques en fonction du processus organisationnel défini, un suivi et une revue des risques doivent être établis tout au long du cycle de vie du système d'IAG.

7. Au besoin, appuyer la démarche de gestion des risques sur un **cadre standardisé de gestion des risques (par exemple, le NIST AI RMF 100 et 600)** pour les cas d'usage ou projets considérés à haut risque par l'OP**.**

Cette démarche doit être proportionnelle aux risques encourus et aux bénéfices liés à l'intégration et à l'utilisation d'un système d'IA, dont les systèmes d'IAG. Elle vise à mettre en place des mesures de mitigation appropriées (considération de la proportionnalité). Parmi les mesures à mettre en place, l'OP doit :

- obtenir et documenter les consentements lorsque requis, notamment lorsqu'il s'agit de renseignements personnels sensibles;
- s'assurer de respecter tous les critères et modalités établis par le Règlement sur l'anonymisation des renseignements personnels (RLRQ, chapitre A-2.1, r. 0.1);

[9] *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c. A -2.1, art. 63.5.
[10] L'ÉFVP, c'est l'évaluation des facteurs relatifs à la vie privée; l'ÉFVP-R est l'outil que propose le MCN pour l'évaluation des facteurs relatifs à la vie privée et des risques.

- s’assurer de la conformité avec le principe de la souveraineté des données utilisées par les solutions d’IAG, c’est-à-dire hébergées au Québec ou dans des juridictions dont la législation est équivalente ou supérieure à celle du Québec en matière de protection des données. Toute exception à cette règle doit être dûment justifiée et documentée, en conformité avec les exigences légales et les principes de souveraineté numérique (Principe de la souveraineté numérique);
- avoir l’avis de sécurité du système d’IAG;
- privilégier l’utilisation d’un système d’IAG avec un modèle ouvert[11] lorsque le contexte exige une traçabilité complète et une reproductibilité des résultats, notamment s’il touche des services destinés aux citoyens ou aux entreprises (Principe de l’explicabilité) quand les cas d’usage impliquent des données confidentielles;
- sensibiliser et former régulièrement le personnel sur les risques et aux bonnes pratiques d’utilisation des systèmes d’IAG.

Il est également recommandé de :

- sensibiliser et former régulièrement le personnel sur les risques liés aux fuites de renseignements confidentiels;
- établir un plan d’action documenté et testé dans le but d’atténuer ou de limiter la survenance des incidents de confidentialité des informations avec des délais de réponse définis;
- encadrer l’utilisation de renseignements confidentiels dans les requêtes aux systèmes d’IAG selon leur niveau de protection :
    - Protégé C (Secret, Très secret) : Interdit dans tous les systèmes d’IAG publics et en circuit fermé; obligatoire dans les systèmes d’IAG gouvernementaux en circuit fermé.
    - Protégé B (Confidentiel) et Protégé A (Diffusion restreinte) : interdit dans les systèmes d’IAG publics; permis dans les systèmes d’IAG en circuit fermé (gouvernemental ou souverain).
    - Non classifié (Public) : Permis dans tous les systèmes d’IAG.
- utiliser et maintenir des filtres automatiques pour empêcher l’envoi non autorisé de renseignements confidentiels;
- héberger les systèmes d’IAG sur des serveurs internes sécurisés, lorsque techniquement et financièrement possibles;
- prioriser, si possible, les cas d’usage d’un système d’IAG qui visent l’amélioration des processus internes avant l’utilisation de celui-ci dans le cadre de la prestation de services publics aux citoyens et entreprises.

[11] 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.

Exemple d'application

Un OP peut assurer sa conformité à la mesure applicable 1.2 en démontrant son application de la démarche d'évaluation des risques proposée dans ce guide, notamment en réalisant une ÉFVP-R et en obtenant un avis de sécurité favorable avant d'utiliser un système d'IAG, ainsi qu'en assurant la mise en place des mesures adéquates pour mitiger les risques établis.

Exemples relatifs à la gestion du risque dans un cycle de vie des systèmes d'IAG :

Phase	Obligations	Recommandations
Conception	Évaluation des risques, choix de la solution souveraine	
Expérimentation		Réalisation de projets pilotes à l'interne, validation à l'interne des hypothèses, et de la sécurité Ajustement des processus avant le déploiement Tests de robustesse
Acquisition	Conformité légale	Justification du fournisseur
Développement	Formation du personnel	Tests de robustesse
Déploiement	Supervision humaine, contrôle des accès	
Exploitation	Surveillance continue, mise à jour des mesures de sécurité	
Mise hors service	Gestion des données, traçabilité, suppression conforme	

Exemple de gestion des risques :

Étape/Obligation	Description/Outil recommandé
Évaluation du degré d'appropriation de l'IA par l'OP	Outil d'évaluation du MCN
Documentation et analyse des besoins d'affaires	Gabarit du portefeuille des occasions en IA
Priorisation des occasions porteuses en IA	Pondération des risques organisationnels
Analyse approfondie de chaque catégorie de risque	Outil ARP, outil ÉFVP-R du MCN
Acceptation des risques résiduels et documentation de la décision	Avant déploiement

1.3. Mise en place de mécanismes de contrôle des systèmes d'IAG

Un organisme public doit 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.

Ce processus doit intégrer des mécanismes de contrôle proportionnels aux risques encourus par l'utilisation des systèmes d'IAG. Cela signifie qu'ils doivent permettre de reconnaître rapidement les risques qui se matérialisent de façon à faciliter la mise en place des mesures préventives et correctives adéquates pour assurer l'efficacité et la sécurité des systèmes d'IAG au sein de l'OP.

De façon générale, un OP peut, au regard des risques résiduels, appliquer les mesures de contrôle suivantes :

- Établir et appliquer un processus de rétroaction structuré pour encourager les utilisateurs à signaler leurs besoins, les obstacles encourus (ex. : hallucinations, biais, etc.) et leurs préoccupations. Par la suite, ajuster le cadre de gouvernance et mettre en place des actions correctives en fonction des signalements émis, le cas échéant;
- Prévoir des mécanismes de révision périodique permettant de s'adapter aux évolutions technologiques;
- Surveiller comment la productivité, la prise de décision et l'innovation au sein de l'OP sont affectées par les impacts ciblés lors de l'évaluation des impacts organisationnels du système d'IAG;

- S’assurer de la fiabilité et la robustesse des systèmes d’IAG, tant avant leur déploiement qu’au cours de leur utilisation, et notamment faire des essais qui incluent la validation du comportement du système face à des demandes qui pourraient générer des réponses erronées (hallucinations, biais) ou face à des demandes auxquelles il ne devrait pas répondre.

Exemple d’application

Un OP peut assurer sa conformité à la mesure applicable 1.3 en désignant une unité responsable de suivre la performance des systèmes d’IAG et en établissant un processus permettant aux utilisateurs de signaler les problématiques rencontrées lors de leur utilisation.

Les types de vérification suivants pourraient être considérés :

- Avant tout déploiement et au cours de leur utilisation, procéder à des essais rigoureux pour vérifier la fiabilité et la robustesse des systèmes d’IAG;
- Audit de sécurité;
- Audit de conformité juridique (ex. : protection des renseignements personnels, protection des droits de propriété intellectuelle, etc.);
- Audit de performance et de qualité des résultats;
- Audit de durabilité et d’impact environnemental (ex. : consommation d’énergie);
- Audit de responsabilité et gouvernance (ex. : contrôle humain).

2. GESTION ET PROTECTION DES DONNÉES NUMÉRIQUES GOUVERNEMENTALES EN VUE DE L'UTILISATION DES SYSTÈMES D'IAG

2.1. Gestion adéquate des DNG utilisées dans les cas d'usage des systèmes d'IAG tout au long de leur cycle de vie

Pour gérer adéquatement le cycle de vie des DNG utilisées dans les cas d'usage ciblés et priorisés par l'OP dans des systèmes d'IAG, il est recommandé de mettre en place une série de mesures :

- Les mesures préparatoires pour appuyer le cycle de vie des DNG au sein des systèmes d'IAG :
    - Mettre en place un système de gestion documentaire structuré, à jour et vérifié;
    - Maintenir une arborescence logique et intuitive de la structure des données;
    - Supprimer les versions obsolètes des données;
    - Éviter les données en double;
    - Optimiser l'organisation documentaire avec des métadonnées et des catégories standardisées;
    - Établir et appliquer des processus de conservation et de suppression conformes au calendrier de conservation exigé par la *Loi sur les archives* (RLRQ, c. A-21.1).

- Les mesures à appliquer tout au long du cycle de vie des DNG au sein des systèmes d'IA :
    - Dresser et tenir à jour un inventaire exhaustif des DNG utilisées par les systèmes d'IAG et documenter leurs métadonnées;
    - Traiter (c'est-à-dire collecter, utiliser, conserver, et/ou communiquer) uniquement les renseignements personnels nécessaires à ces cas d'usage;
    - S'assurer de la qualité et de la cohérence des DNG utilisées par les systèmes d'IAG;
    - Protéger les renseignements personnels lors de l'utilisation d'un système d'IAG.

- La surveillance de l'utilisation, de la protection et de la qualité des DNG, de même que de leur transformation par les systèmes d'IAG, est cruciale.
    - Maintenir les systèmes d'IAG dans des environnements conformes à la classification des DNG traitées :

- pour les systèmes d'IAG publics : utiliser uniquement des DNG non classifiées (publiques) et être conscient que les données soumises peuvent être utilisées pour l'entraînement ou l'amélioration des modèles;
- pour les systèmes d'IAG en circuit fermé (souverain ou gouvernemental) : s'assurer que les mesures contractuelles et techniques appropriées sont en place pour protéger les DNG selon leur classification, incluant des garanties sur l'utilisation, la conservation et la non-exposition des données lors de l'entraînement ou de l'ajustement des modèles d'IAG.

Exemple relatif à la gestion et à la protection des DNG :

Mesure	Phase/Moment d'application
Mettre en place un système de gestion documentaire structuré, à jour et vérifié	Préparatoire
Maintenir une arborescence logique et intuitive de la structure des données	Préparatoire
Supprimer les versions obsolètes des données	Préparatoire
Éviter les données en double	Préparatoire
Optimiser l'organisation documentaire avec des métadonnées et des catégories standardisées	Préparatoire
Établir et appliquer des processus de conservation et de suppression conformes au calendrier légal	Préparatoire
Dresser et tenir à jour un inventaire exhaustif des DNG utilisées par les systèmes d'IAG	Tout au long du cycle de vie
Traiter uniquement les renseignements personnels nécessaires	Tout au long du cycle de vie
S'assurer de la qualité et de la cohérence des DNG utilisées	Tout au long du cycle de vie
Protéger les renseignements personnels lors de l'utilisation d'un système d'IAG	Tout au long du cycle de vie

2.2. Classification[12] et sécurisation des DNG avant leur utilisation dans les cas d'usage des systèmes d'IAG

Avant toute utilisation des DNG utilisées dans les cas d'usage des systèmes d'IAG, chaque OP doit s'assurer notamment :

- d'appliquer le Modèle de classification de sécurité des données numériques gouvernementales approuvé par le MCN pour protéger les DNG utilisées dans chaque cas d'usage;
- de mettre en œuvre des mesures de sécurité garantissant la souveraineté des données selon l'analyse des préjudices et la classification des DNG traitées par un système d'IAG, en respectant les règles suivantes :
  - Protégé C (Secret, Très secret) : Utilisation obligatoire d'un système d'IAG gouvernemental en circuit fermé uniquement;
  - Protégé B (Confidentiel) et Protégé A (Diffusion restreinte) : Utilisation interdite dans les systèmes d'IAG publics; permise uniquement dans les systèmes d'IAG en circuit fermé (souverain ou gouvernemental);
  - Non classifié (Public) : Utilisation permise dans tous les types de systèmes d'IAG.

Exemple : Matrice de souveraineté pour l'hébergement et le traitement des DNG :

Utilisation encadrée des systèmes d'IAG publics

Confidentialité de l'information soumisse ou produite dans l'IAG	Cas d'usage / exemples	IAG publique *(ex.: ChatGPT, MS Copilot, Claude)*	IAG circuit fermé *(ex.: MS Copilot Entreprise)*	IAG souveraine *IAG privée, immunisée aux législations étrangères, et hébergée au Canada*	IAG gouvernementale en circuit fermé *IAG privée, gérée et hébergée dans un CTI gouvernemental*
Non classifié Public	• Information en provenance ou destination du web public • Code applicatif sous licence publique	Permis	Permis	Permis	Permis
Protégé A Diffusion restreinte	• Code applicatif privé • Note interne	Interdit	Permis	Permis	Permis
Protégé B Confidentiel	• Renseignement personnel • Note stratégique	Interdit	Permis	Permis	Permis
Protégé C Secret, Très secret	• Renseignement personnel sensible • Note hautement stratégique	Interdit	Interdit	Interdit	Obligatoire

[12] Arrêté numéro 2024-05 du ministre de la Cybersécurité et du Numérique en date du 12 décembre 2024 concernant le Modèle de classification de sécurité des données numériques gouvernementales (84711.pdf).

2.3. Gestion des accès aux DNG pour assurer un contrôle strict des droits d'accès aux données et aux systèmes d'IAG

Pour assurer un contrôle strict de l'accès aux données par les systèmes d'IAG, l'OP doit s'assurer notamment :

- d'appliquer les principes de sécurité reconnus (Principe de la sécurité);
- de réviser périodiquement les autorisations d'accès aux DNG requises par les cas d'usage des systèmes d'IAG;
- d'encadrer strictement l'accès aux systèmes d'IAG en le réservant aux usages autorisés par les politiques internes de l'OP et aux personnes expressément habilitées et autorisées;
- d'établir et d'appliquer des mécanismes d'authentification forte et des protocoles d'accès sécurisés;
- de vérifier régulièrement les contrôles d'accès basés sur les rôles;
- de mettre en place un système de traçabilité détaillée des accès aux renseignements confidentiels;
- de vérifier et de renforcer les mécanismes de journalisation et de surveillance pour détecter toute activité suspecte et pour répondre aux audits internes ou externes et aux obligations légales (notamment celles prévues par la LAI, la LCCJTI, la LGGRI, et la LRSSS);
- de définir des quotas d'utilisation et de surveiller les requêtes anormales en temps réel;
- de vérifier et de renforcer les niveaux d'autorisation pour limiter les modifications des données sensibles.

L'OP doit respecter les exigences en matière de ressources informationnelles, telles que :

- La validation régulière que les systèmes d'IAG demeurent fiables et sécuritaires, conformément aux obligations en matière de sécurité de l'information;
- Des tests de robustesse et d'intrusion pour valider la résistance aux attaques et aux manipulations (ex. : rédactique (*prompt engineering*));
- Une surveillance continue pour détecter rapidement toute dérive ou comportement inattendu;
- Des mécanismes de repli et un plan de continuité des activités en cas de défaillance.

Exemple concret d'application — Mise en place d'un système d'IAG dans un OP

Un OP souhaite déployer un système d'IAG pour automatiser le traitement de demandes citoyennes. Ce système aura accès à des DNG, dont des renseignements personnels.

- L'OP intègre la gouvernance des systèmes d'IAG dans sa structure existante et s'appuie également sur la gouvernance des DNG déjà en place (réf. : ligne 1.1);
- L'OP réalise une série de mesures préparatoires sur ses DNG avant le déploiement du système d'IAG (réf. ligne 2.1);
- L'OP suit un processus d'approbation et de suivi des cas d'usage (réf. : ligne 1.1);
- L'OP suit des mesures de protection et de valorisation des données :
    - les renseignements personnels nécessaires de chaque cas d'usage des systèmes d'IA sont uniquement traités;
    - les principes de sécurité reconnus (gestion fine des habilitations, traçabilité des accès, chiffrement, procédures en cas d'incident) sont appliqués par l'OP pour l'ensemble de ses systèmes d'IA (Principe de la sécurité);
    - les données sont valorisées (identification des données à valeur stratégique à l'organisme, optimisation de leur organisation et de leur qualité pour améliorer les services publics);
- L'OP veille à mettre en place des activités de communication et de formation en lien avec le système d'IA (réf. : lignes 3.1 et 3.2).

Exemple : Dispositifs de supervision humaine et contrôle

Dispositif	Obligatoire	Description
Validation avant actions critiques	✓	Processus de vérification humaine avant décision
Mécanisme d'arrêt d'urgence	✓	Arrêt immédiat du système en cas de dérive
Suivi en temps réel des décisions	✓	Outils de suivi et traçabilité
Documentation des interventions	✓	Journalisation des actions et validations humaines

3. INTÉGRATION ET UTILISATION RESPONSABLES DES SYSTÈMES D'IAG PAR LE PERSONNEL DES ORGANISMES PUBLICS

3.1. Compétences du personnel et sensibilisation aux risques associés aux systèmes d'IAG

Un programme formel de formation et de sensibilisation en matière d'IA doit être mis en œuvre par l'OP avant de mettre un système d'IAG à la disposition de son personnel (Principe de la compétence). De plus, l'OP doit assurer une gestion du changement proportionnée à l'impact organisationnel lié à l'introduction d'un système d'IAG, afin de favoriser une intégration optimale de cette technologie.

Ainsi, l'OP doit s'assurer de :

- suivre une méthode d'apprentissage expérientiel où le personnel apprend par l'entremise du déploiement progressif des systèmes d'IAG et des projets pilotes, incluant de la formation et de la sensibilisation;
- fournir une assistance technique accessible;
- établir un plan de gestion du changement pour accompagner le personnel;
- ajuster les formations et processus système.

Le programme doit inclure minimalement les formations que peut proposer le ministère de la Cybersécurité et du Numérique. Ces formations sont notamment (si disponible et sans s'y limiter) :

  - Introduction à l'intelligence artificielle dans l'administration publique
  - L'intelligence artificielle générative : opportunités, risques et défis
  - Le marquage des données numériques gouvernementales

Exemple d'application

Un OP peut assurer sa conformité à la mesure applicable 3.1 en procédant à un lancement progressif du système d'IAG et des projets pilotes qui ciblent des directions spécifiques de l'organisation et qui permettent l'ajustement des formations et des processus en fonction des résultats observés.

Exemple d'un plan de formation :

Formation	Proposée par le MCN (obligatoire)	Catalogue centralisé	Personnalisable par l'OP	Commentaires
Introduction à l'intelligence artificielle dans l'administration publique	✓	✓	✓	Pour tous les employés autorisés
IA générative : opportunités, risques et défis	✓	✓	✓	Sensibilisation aux enjeux
Le marquage des données numériques gouvernementales	✓	✓	✓	Protection des données
Formation complémentaire (ex. éthique, sécurité avancée)		Selon les besoins de l'OP		

3.2. Compétences du personnel pour traiter et appliquer de manière responsable les cas d'usages des systèmes d'IAG privilégiés par un OP

De façon générale, il est demandé à l'OP de promouvoir l'utilisation responsable des systèmes d'IAG par des pratiques respectueuses, notamment des droits de propriété intellectuelle, du droit à la vie privée, de la protection des renseignements personnels et du principe de la transparence. Pour cela, les OP s'assurent que leur personnel connaît minimalement les bonnes pratiques présentées dans le présent guide et qu'il les applique lorsque la situation le requiert.

De façon générale, il est important de mettre en place ou de rendre accessibles des formations ou toutes autres mesures jugées adéquates par l'OP.

L'OP doit :

- sensibiliser le personnel à la qualité et à la validité de l'information produite par les systèmes d'IAG et à l'importance de la vérification systématique des résultats;
- développer la capacité du personnel à valider la fiabilité et la pertinence des réponses des systèmes d'IAG;
- sensibiliser le personnel au fonctionnement des systèmes d'IAG, à ses capacités, à ses forces, à ses limitations et à ses enjeux;

Il est également recommandé de :

- former le personnel aux techniques de rédactique (formulation d'une requête) dans le but d'obtenir des résultats plus pertinents aux requêtes envoyées à un système d'IAG;
- développer la capacité du personnel à comprendre et à éviter les biais pour garantir des résultats équitables;
- former le personnel à utiliser la pensée critique et son expertise pour l'évaluation critique des contenus générés et à la diversification des sources d'information.

Exemple d'application

Un OP peut assurer sa conformité à la mesure applicable 3.2 en démontrant que son personnel a suivi, sans s'y limiter, une formation sur la sensibilisation aux perspectives, aux risques et aux défis de l'IAG ou une formation équivalente avant d'utiliser un système d'IAG pour leurs cas d'usage.

3.3. Prioriser les cas d'usage et assurer leur mise en œuvre

Les cas d'usage des systèmes d'IAG identifiés par l'OP 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 (Principe de l'efficience, de l'efficacité et de la pertinence) ou à d'autres bénéfices (impacts positifs, gains, réduction des coûts). Il est important de documenter chacun des cas d'usage, 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 identifiés doivent être analysés et priorisés en considérant non seulement les bénéfices anticipés, mais également les risques encourus. Il est recommandé aux organismes publics de s'appuyer sur le **gabarit du portefeuille des occasions porteuses en IA** du MCN.

De façon générale, l'OP applique les mesures suivantes dans le processus d'analyse et de priorisation des cas d'usage ciblés.

L'OP doit :

- prioriser les cas d'usage ou processus d'affaires pour assurer un rendement avant le déploiement;
- privilégier l'utilisation de modèles ouverts dans les systèmes d'IAG afin de faciliter l'explicabilité et la transparence des résultats (Principe de l'explicabilité). Il est essentiel de fournir des explications claires et compréhensibles sur le fonctionnement et les décisions des systèmes d'IAG, notamment en documentant les critères appliqués et les mécanismes d'interprétation;
- privilégier l'utilisation de modèles spécialisés (ou vertical) lorsqu'il est disponible et économiquement viable, afin de garantir l'efficience et la qualité des résultats pour les cas d'usage de l'OP (Principe de l'efficience, de l'efficacité et de la pertinence);
- identifier des cas d'usage interdits ou soumis à des restrictions;
- privilégier les systèmes d'IAG offrant une souveraineté accrue (Principe de la souveraineté numérique);
- identifier soigneusement les systèmes d'IAG sécuritaires pour chaque cas d'usage;
- évaluer régulièrement les impacts sur l'équité et l'inclusion (Principe d'inclusion et d'équité);
- évaluer et surveiller l'impact de l'IAG sur les droits de la personne (Principe du respect des personnes et de la règle de droit);
- assurer la protection des renseignements confidentiels;
- avoir les capacités nécessaires pour assurer les formations, la supervision humaine des résultats des systèmes d'IAG (Principe de l'autonomie et de la supervision humaine) et du déploiement de ces systèmes;

Il est également recommandé de :

- Définir dans quels contextes l'utilisation d'un système d'IAG peut apporter de la valeur; prioriser l'intégration des systèmes d'IAG dans les emplois de soutien administratif et pour les emplois impliquant une grande portion de rédaction et de révision de document (ex. : rédaction et synthèse, assistance à la créativité, analyse et structuration des données, soutien client et FAQ, etc.);

- Mettre des efforts pour l'automatisation, l'exploration et l'intégration des systèmes d'IAG afin de permettre des gains tangibles sur le plan financier;
- Prioriser, lorsque possible, des fournisseurs dont les pratiques sont responsables d'un point de vue social et environnemental (Principe de la durabilité) selon les informations et la documentation disponible de la part des fournisseurs;
- Éviter les usages non essentiels, privilégier les modèles légers et économes en énergie selon les spécifications techniques et la documentation disponible de la part des fournisseurs;
- Optimiser la consommation énergétique et sensibiliser les utilisateurs à l'impact carbone;
- Encourager la réutilisation et la mutualisation des systèmes d'IAG et requêtes;
- S'assurer que le programme de formation permet de responsabiliser les utilisateurs sur le principe de durabilité;
- Mettre en place un suivi et des indicateurs de durabilité;
- Documenter l'utilisation des systèmes d'IA en indiquant les requêtes et réponses associées accessibles par le personnel pour obtenir le résultat souhaité par le personnel;
- Des processus de validation avant toute action ou décision critique;
- Mettre en place des mécanismes d'arrêt d'urgence;
- Prévoir des outils de suivi en temps réel des décisions prises par le système.
- Vérifier la compatibilité des licences avec un usage gouvernemental.

Exemple d'application

Un OP peut démontrer sa conformité à la mesure applicable 3.3 en maintenant un registre complet et à jour des cas d'usage autorisés et en cours d'évaluation. Ce registre doit documenter de façon rigoureuse chaque cas d'usage en identifiant clairement les données utilisées et les accès requis.

Sont également consignés, pour chaque cas d'usage identifié par l'OP, les impacts potentiels du système d'IAG sur l'équité, l'inclusion et les droits de la personne. Par exemple :

- **Équité et inclusion** : si les informations produites par le système d'IAG risquent de porter préjudice à un groupe vulnérable (par exemple, en raison de données biaisées ou d'un algorithme d'entraînement biaisé), ces risques doivent être relevés et suivis.
- **Droits de la personne** : si le système d'IAG risque de générer des informations erronées en lien avec un service public, et que celles-ci ne respectent pas la législation en vigueur, l'impact doit être identifié et des mesures correctives doivent être appliquées.

4. UNE UTILISATION ENCADRÉE DES SYSTÈMES D'IAG PUBLICS[13]

4.1. Utilisation des systèmes d'IAG publics limitée aux cas d'usage autorisés

Un OP doit prioriser l'utilisation de systèmes d'IAG privés et sécurisés plutôt que des systèmes d'IAG publics, afin de garantir la confidentialité et l'intégrité des renseignements de l'OP.

Un OP peut en tout temps interdire l'utilisation des systèmes d'IAG publics au sein de son organisation. Néanmoins, si cette utilisation est permise, l'OP doit s'assurer que le personnel l'utilise de façon responsable et sécuritaire, et cela, dans les limites autorisées par les autorités compétentes.

Un OP doit interdire au personnel d'utiliser des renseignements de nature confidentielle dans un système d'AIG public.

Étant donné la grande variété des cas d'usage possibles et des systèmes d'IAG disponibles publiquement, il est demandé aux OP d'adopter des règles internes définissant le type d'utilisation acceptable ainsi que les systèmes d'IAG publics autorisés, et ce, en concordance avec les lois et les textes d'application en vigueur au Québec. Ces balises doivent s'appuyer sur une évaluation des risques et la limitation de l'utilisation des systèmes d'IAG publics qu'à des cas d'usage conformes au niveau de risques acceptés par l'OP.

Bien qu'il existe plusieurs façons d'établir des balises d'utilisation d'une technologie, il est demandé d'adopter un encadrement interne. L'OP peut se référer au *Guide des bonnes pratiques pour une utilisation de l'IA générative dans l'administration publique* pour définir des balises adaptées à leur organisation.

Comme pour les systèmes d'IAG privés, les organismes publics s'assurent de former et de sensibiliser leur personnel à l'utilisation responsable[14] des systèmes d'IAG publics (réf. : lignes 3.1 et 3.2) et de désigner une unité responsable pour le suivi de l'utilisation des systèmes publics (réf. : ligne 1.1).

---

[13] Système d'IAG public : toute version « grand public » gratuite ou non de systèmes d'IA générative, comme les versions en ligne de Copilot (incluant Copilot Chat) et ChatGPT, accessible par le web à l'extérieur de l'organisation, pour autant qu'elle ne soit pas interdite par celle-ci.

[14] Une utilisation responsable de l'IA est une utilisation qui respecte l'*Énoncé de principes pour une utilisation responsable de l'intelligence artificielle par l'OP.*

Exemple d'application

Un OP peut démontrer sa conformité à la mesure applicable 4.1 en interdisant l'utilisation des systèmes d'IAG publics ou en instaurant une directive interne limitant le recours à ces systèmes pour des types d'utilisation précis. La désignation d'une unité responsable du maintien des règles à jour selon l'évolution technologique est également essentielle.

Type d'usage	Systèmes d'IAG publics permis	Conditions/Restrictions
Rédaction de contenu non sensible	✓	Aucun renseignement confidentiel ou stratégique
Reformulation, traduction, correction	✓	Texte public ou non classifié
Aide à la programmation (code anonymisé)	✓	Pas de données personnelles ou stratégiques
Automatisation de tâches dans outils approuvés	✓	Utiliser uniquement des outils infonuagiques validés par l'organisation
Génération de documents publics	✓	Ne pas inclure d'information interne ou confidentielle
Transmission de renseignements confidentiels	X	Interdiction absolue
Traitement de données sensibles/stratégiques	X	Interdiction absolue
Décisions automatisées sans supervision humaine	X	Superviser toute décision impactant un citoyen
Réentraîner le modèle sur des sorties non validées	X	Risque d'amplification des biais ou erreurs

Cybersécurité
et Numérique
Québec