AUTORITÉ DES MARCHÉS PUBLICS | TRANSPARENCE ÉQUITÉ SAINE CONCURRENCE

CADRE DE GESTION DE L'INFORMATION

Avril 2024

TABLE DES VERSIONS

Version	Nature des changements	Élaboré par :	Date d'adoption
1.0	Version initiale – Cadre de gouvernance de l'information	Secrétariat général	Février 2023
2.0	Bonification de la section Protection des renseignements personnels	Secrétariat général	Septembre 2023
2.1	Modification du titre du document et des textes relatifs à la gouvernance	Secrétariat général	Avril 2024

TABLE DES MATIÈRES

1. INTRODUCTION

L'Autorité des marchés publics (l'« AMP ») produit, utilise et reçoit une quantité importante d'informations essentielles à la réalisation de sa mission, qui constitue son actif informationnel.

La gestion de cet actif nécessite la mise en place d'une structure de gouvernance comportant des processus, une définition des rôles et responsabilités, des outils de contrôle et des indicateurs permettant d'en assurer une gestion efficace et efficiente.

L'AMP reconnaît que l'atteinte de ses objectifs est tributaire de la saine gestion de son information. De plus, la gestion transparente et optimale de l'information contribue à établir la confiance du public envers l'organisation, démontre sa capacité à mettre en œuvre son savoir-faire et permet de préserver sa crédibilité ainsi que sa réputation.

L'information subit un important virage au numérique. La saine gestion de celle-ci facilite l'adaptation aux changements technologiques et permet de gérer adéquatement la masse documentaire sous toutes ses formes.

Par conséquent, l'AMP souhaite promouvoir et développer une culture organisationnelle proactive en matière de gestion et de gouvernance de l'information.

La gouvernance de l'information se définit comme une approche stratégique, dont la mise en œuvre repose sur huit principes directeurs communément admis[1], soient : la responsabilité, la transparence, l'intégrité, la protection, la conformité, la disponibilité, la conservation et la disposition.

L'application et l'opérationnalisation de ces principes directeurs à travers les activités courantes de l'AMP engendrent une gestion de l'information unifiée, qui permet de mieux valoriser, créer, classer, utiliser et partager cette information.

2. OBJET

Le présent cadre de gestion a pour objet d'établir les principes de base de la structure de gouvernance de l'information de l'AMP. Il définit les rôles et les responsabilités nécessaires à une saine gestion de l'information.

Ce cadre instaure une approche multidisciplinaire cohérente au sein de l'AMP, qui se décline selon les volets suivants:

- La gestion de l'information et des documents
- L'accès à l'information
- La protection des renseignements personnels
- La sécurité de l'information

3. CHAMP D'APPLICATION

Le cadre de gestion de l'information s'applique à l'ensemble du personnel de l'AMP.

[1] The Generally Accepted Recordkeeping Principles (GARP), ARMA, https://www.arma.org/page/principles

4. DÉFINITIONS

Pour les fins du présent document, les termes suivants sont définis comme suit :

Calendrier de conservation Outil archivistique établissant les délais de conservation fixés pour l'ensemble des documents d'un organisme et qui établit pour chaque série documentaire lesquelles seront éliminées ou conservées pour leur valeur historique.	**Cycle de vie du document** Ensemble des étapes franchies par un document, depuis sa création, en passant par son transfert, sa consultation et sa transmission, jusqu'à sa conservation, y compris son archivage ou sa destruction.
Document Toute information consignée sur quelque support que ce soit, incluant toute banque de données permettant la création de documents et la structuration de l'information qui y est inscrite.	**GID** Gestion de l'information et des documents.
Plan de classification Structure hiérarchique et logique constituée de rubriques dans lesquelles sont présentées les processus et activités d'une organisation et qui permet la classification, le classement et le repérage de documents et de dossiers.	**Protection des renseignements personnels** Ensemble des mesures visant à protéger les renseignements personnels collectés, utilisés, communiqués, conservés ou détruits dans le cadre des activités de l'organisme, contre une utilisation non autorisée, inappropriée ou illégale pouvant porter atteinte au droit à la vie privée de la personne concernée.
Sécurité de l'information Ensemble de mesures visant à protéger des informations et des données, en fonction de leur niveau de disponibilité, d'intégrité et de confidentialité.	**Sécurité informatique** Ensemble de mesures physiques, logiques et administratives pour assurer la sécurité des biens informatiques, la confidentialité des données de son système d'information et la continuité de son service. La sécurité informatique est l'une des composantes de la sécurité de l'information.

5. CADRE LÉGAL

Le présent cadre de gestion s'inscrit dans un contexte régi principalement par :

- La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c. A-2.1
- La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*, RLRQ, c. G-1.03
- La *Loi favorisant la transformation numérique de l'administration publique*, RLRQ, c. T-11.003
- La *Loi sur les archives*, RLRQ, c. a-21.1
- La *Loi concernant le cadre juridique des technologies de l'information*, RLRQ, c. C-1.1
- Le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels*, c. A-2.1, r.2
- La *Directive gouvernementale sur la sécurité de l'information*, décret 1514-2021
- La *Charte des droits et libertés de la personne*, RLRQ, C-12
- Le *Code civil du Québec*

6. COMITÉ SUR LA PROTECTION DE L'INFORMATION

Le comité sur la protection de l'information a été fondé conformément à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (« Loi sur l'accès »). Relevant du président-directeur général de l'AMP, il doit soutenir celui-ci dans l'exercice de ses responsabilités et de ses obligations en vertu de cette loi.

Ce comité répond également à l'obligation de la *Directive gouvernementale sur la sécurité de l'information*, qui prévoit qu'un organisme public doit mettre en place un comité de travail approprié de coordination et de concertation en matière de sécurité de l'information. Il établit une approche multidisciplinaire de la protection de l'information.

Son mandat est de traiter les enjeux organisationnels relatifs à l'accès à l'information, à la protection des renseignements personnels et à la sécurité de l'information. Il doit notamment approuver les règles de gouvernance relatives à ces aspects, suivre l'avancement des plans d'action établis et être consulté sur l'évaluation des facteurs relatifs à la vie privée qui doit être réalisée pour certains projets.

Le comité se compose des personnes suivantes, qui peuvent être accompagnées de leurs collaborateurs lors des rencontres :

- Le secrétaire général, responsable de l'accès aux documents et de la protection des renseignements personnels et de la gestion documentaire;
- Le directeur principal du soutien organisationnel;
- La directrice des technologies de l'information, responsable de la sécurité de l'information et de la sécurité informatique.

Lorsqu'un sujet requiert une expertise particulière, les membres du comité peuvent inviter tout autre participant.

7. SENSIBILISATION ET FORMATION DU PERSONNEL

La sensibilisation et la formation du personnel aux enjeux relatifs à la gestion de l'information favorisent l'adhésion et la mobilisation de celui-ci. L'implication de tous, à différents niveaux, améliore la cohérence des actions posées et réduit les risques d'incidents relatifs à la gestion de l'information.

L'AMP incite le partage et la mise à jour de connaissances entre les membres du personnel qui possèdent une expertise dans les champs de compétences reliés à la gestion de l'information.

8. ENCADREMENTS

L'AMP a mis en place un cadre de gestion interne qui permet de guider les actions de son personnel relativement aux différents aspects de la gestion de l'information. Les encadrements suivent l'évolution des différentes obligations légales des organismes publics et font l'objet de révisions périodiques afin d'en assurer leur exactitude.

9. REDDITION

L'AMP effectue une reddition de comptes et publie les renseignements liés à sa gouvernance de l'information, à l'intérieur de son rapport annuel d'activités :

Accès à l'information et protection des renseignements personnels

- Nombre total de demandes d'accès à l'information reçues
- Nature des demandes traitées
- Délais de traitement
- Nombre d'avis de révision reçus de la Commission d'accès à l'information
- Activités du comité fondé conformément à la Loi sur l'accès
- Encadrements adoptés

GID

- Activités réalisées dans le cadre du déploiement du programme de gestion de l'information et des documents

De plus, conformément aux exigences de la *Loi sur la gouvernance et la gestion des ressources informationnelles*, l'AMP réalise des bilans spécifiques en sécurité de l'information.

PRINCIPES DIRECTEURS

10. PRÉSENTATION ET DÉFINITION DES PRINCIPES DIRECTEURS

L'architecture de gouvernance de l'information de l'AMP repose sur huit principes directeurs[2], communément admis en gestion de l'information et des documents.

Afin d'améliorer continuellement les pratiques relatives à la gestion de l'information, ces principes directeurs doivent être considérés lors de la prise de décisions ayant un impact sur la gestion de l'actif informationnel de l'AMP et doivent être incorporés aux activités courantes de l'organisation.

Responsabilité

La gouvernance de l'information doit relever de la haute direction et être supervisée par celle-ci. Le déploiement du cadre de gestion est confié à des personnes désignées. L'organisation doit adopter des processus, directives et règles de conduite qui guident le personnel et assurent la conformité du cadre de gestion.

- La haute direction de l'AMP doit adhérer aux orientations proposées en gouvernance de l'information et favoriser la participation des différents intervenants à l'interne.
- Les encadrements adoptés doivent permettre au personnel de comprendre leurs rôles et leurs responsabilités relatives à la gestion de l'information.

Transparence

L'information relative aux activités d'affaires et au déploiement du cadre de gestion de l'information dans l'organisation doit être documentée de manière ouverte. Elle est accessible pour les parties prenantes et le personnel impliqué.

- La collaboration à l'interne entre les parties prenantes nécessite que chacune d'entre elles comprennent son propre rôle, mais également celui des autres afin d'agir de manière concertée.

Intégrité

Le cadre structure la gestion de l'information et des documents produits, utilisés et reçus de manière à assurer leur authenticité et leur fiabilité.

- Les systèmes et les solutions logicielles utilisés à l'AMP doivent permettre l'intégration de métadonnées et garantir de manière raisonnable la crédibilité, l'exhaustivité, l'exactitude et l'authenticité de l'information gérée.

Protection

Le cadre de gestion doit être construit de manière à assurer un niveau raisonnable de protection de l'information et des données qui sont privées, confidentielles, privilégiées, secrètes ou essentielles à la continuité de l'organisation.

- La protection de l'information doit être une préoccupation importante et constante au sein de l'AMP.

[2] ARMA, *The Generally Accepted Recordkeeping Principles (GARP*), https://www.arma.org/page/principles

- L'AMP doit catégoriser ses actifs informationnels afin de déterminer la valeur de ceux-ci, ainsi que le niveau de protection requis pour chacune des catégories.
- Les droits d'accès aux systèmes doivent être limités aux moindres privilèges, de manière à réduire le risque d'utilisation non autorisée.

Conformité

Le cadre de gestion de l'information établi doit permettre d'assurer le respect des exigences législatives, règlementaires et gouvernementales.

- L'AMP doit s'assurer d'effectuer une vigie des nouvelles lois, règlements et obligations en matière de gestion et de gouvernance de l'information.
- Les processus et encadrements en place doivent permettre de maintenir la conformité de façon continue.

Disponibilité

L'information doit être enregistrée et classée afin qu'elle puisse être repérée rapidement, efficacement et avec précision.

- Le plan de classification établi doit être appliqué par l'ensemble du personnel, afin de cartographier adéquatement l'actif informationnel de l'AMP.
- L'enregistrement de l'information et des documents doit se faire de manière ordonnée, à l'endroit approprié.

Conservation

L'information doit être conservée durant une période déterminée.

- Le délai de conservation de l'information doit être établi à partir des caractéristiques relatives à celle-ci, notamment du point de vue historique, légal et opérationnel.
- Le calendrier de conservation de l'AMP doit être appliqué de façon diligente et continue, afin que l'information et les documents ne soient conservés que pour la période appropriée.

Disposition

L'organisation doit s'assurer que la disposition de l'information et des documents se fait de manière appropriée et conformément au cadre normatif applicable.

- La destruction des documents doit être faite en conformité avec le calendrier de conservation.
- Les documents inactifs devant être archivés doivent être versés une fois par an à Bibliothèque et Archives nationales du Québec.

GESTION DE L'INFORMATION ET DES DOCUMENTS

11. CONTEXTE

La saine gestion de l'information et des documents est essentielle à la réalisation de la mission de l'AMP, en plus de lui permettre de rendre compte de ses activités. Elle permet notamment à l'AMP de colliger adéquatement l'information requise afin de respecter l'ensemble de ses obligations en matière de protection de l'information.

La GID est étroitement liée à l'efficience de l'organisation. Elle permet d'appuyer les processus et la prise de décision basée sur des données fiables. La GID permet la mise en place de bonnes pratiques qui limitent les risques d'altération, de modification involontaire ou de perte d'information utile à la continuité des activités de l'AMP.

Elle est aussi indispensable pour constituer et préserver la mémoire institutionnelle.

Les informations et les documents détenus et utilisés par l'AMP sont gérés en fonction de leur valeur et leurs caractéristiques, tout au long de leur cycle de vie. Le plan de classification établit l'organisation de l'information selon une structure logique, qui facilite le repérage efficace et précis de celle-ci.

L'AMP s'assure de respecter les obligations prévues à la *Loi sur les archives*, qui impliquent notamment l'adoption et la mise à jour d'un calendrier de conservation afin de déterminer les périodes d'utilisation et les supports de conservation des documents.

La GID permet également de veiller à ce que la masse documentaire numérique, en croissance constante, respecte les principes établis dans la *Loi concernant le cadre juridique des technologies de l'information*.

12. PLAN DE CLASSIFICATION

Le plan de classification de l'AMP est son outil principal de classement et d'archivage, qui prévoit une structure hiérarchique et logique de rubriques dans lesquelles sont présentés les processus et activités de l'organisation.

L'information de l'AMP doit être structurée et classée selon le plan de classification.

Il doit être appliqué par l'ensemble du personnel pour assurer une classification appropriée de l'information et des documents.

13. CALENDRIER DE CONSERVATION

Le calendrier de conservation de l'AMP est directement lié aux rubriques de son plan de classification.

Il détermine les durées de conservation des dossiers et documents administratifs, en plus de prévoir leur mode de disposition au terme de leur vie utile.

Le calendrier prévoit le mode de disposition d'un document, soit sa destruction ou son transfert à Bibliothèque et archives nationales du Québec.

14. CYCLE DE VIE DU DOCUMENT

Les éléments qui constituent le cycle de vie d'un document sont :

- La création
- La modification
- Le transfert de l'information
- La consultation
- La transmission
- La conservation
- L'archivage ou la destruction

15. GREFFE

Le greffe de l'AMP est administré par le Secrétariat général.

Il consiste en une voûte documentaire numérique sécurisée qui permet l'archivage de décisions émanant des différentes instances décisionnelles, regroupées sous forme de collections.

Le greffe facilite l'accès aux documents essentiels à la mémoire de l'organisation.

16. RÔLES ET RESPONSABILITÉS

16.1 Dirigeant de l'organisme public

Le président-directeur général approuve les orientations en matière de gestion de l'information et des documents.

16.2 Responsable de la gestion documentaire

La personne responsable de la gestion documentaire relève du Secrétariat général.

Elle doit :

- Analyser la situation de l'organisme afin de déterminer les besoins en gestion documentaire;
- Établir, tenir à jour et mettre en œuvre le programme de GID;
- Déployer et piloter la solution logicielle de gestion documentaire de l'AMP;
- Élaborer, mettre à jour et veiller au respect du plan de classification et du calendrier de conservation;
- Élaborer et offrir de la formation portant sur les principaux outils de gestion documentaire;
- Exercer un rôle-conseil pour l'ensemble du personnel pour les questions relatives aux outils de gestion documentaire;
- S'assurer de l'application du cycle de vie des documents de leur création jusqu'à leur versement à Bibliothèque et archives nationales du Québec ou leur destruction;
- Être partie prenante de toute initiative impliquant la gestion d'information et de documents.

16.3 Secrétariat général

Le Secrétariat général exerce un rôle-conseil en matière de gestion efficiente et de saine gouvernance de l'information et de la protection de l'intégrité organisationnelle. Il rend disponible son expertise pour exercer un support stratégique aux directions et en appui aux projets de l'AMP.

Il est responsable d'élaborer les encadrements qui définissent les pratiques organisationnelles en gestion de l'information et des documents.

16.4 Vice-présidence à l'administration

La Vice-présidence à l'administration est responsable de la gestion de projets.

Elle sollicite la participation du Secrétariat général afin de fournir une expertise en GID pour tout projet de l'AMP qui implique la gestion d'information, de données ou de documents.

Elle est également responsable de mettre en œuvre les outils technologiques et informatiques nécessaires au déploiement du programme de GID. Elle doit :

- Intégrer la GID lors du déploiement des solutions logicielles à l'AMP;
- Participer conjointement avec la responsable de la gestion documentaire à l'évaluation les solutions logicielles en matière de GID;
- Accorder les droits d'accès technologiques déterminés aux dossiers et documents.

16.5 Gestionnaires

Chaque gestionnaire est responsable de s'assurer de l'application du programme de GID établi au sein de sa direction ou son service.

De plus, le gestionnaire doit:

- S'assurer que les membres du personnel de son équipe sont adéquatement formés à l'utilisation des outils de GID, dont le plan de classification et les solutions logicielles en place;
- Gérer les droits d'accès aux dossiers et documents de sa direction ou son service, selon le niveau de sécurité et de confidentialité requis;
- Autoriser les opérations de déclassement et de destruction de documents de sa direction ou son service;
- Informer la responsable de la gestion documentaire de tout changement de responsabilités ou mandats de son équipe, afin d'évaluer l'incidence sur le plan de classification et le calendrier de conservation;
- Solliciter la participation du responsable de la gestion documentaire lors de la planification, l'élaboration ou la réalisation de projets liés à la gestion d'informations, de données ou de documents dans sa direction ou son service.

16.6 Membre du personnel

Chaque membre du personnel doit contribuer au respect des bonnes pratiques de GID mises en place. Le personnel doit :

- Classer l'information et les documents reçus, produits ou utilisés dans le cadre de son travail dans la voûte documentaire, en respectant le plan de classification établi;
- Prendre connaissance des outils de GID mis à sa disposition;
- Participer aux formations en GID;
- Laisser sous la garde de l'organisation tous les documents produits, reçus ou utilisés.

ACCÈS À L'INFORMATION

17. CONTEXTE

La *Charte des droits et libertés de la personne* prévoit que toute personne a droit à l'information, dans la mesure prévue par la loi. L'exercice de ce droit implique notamment que chaque personne doit pouvoir accéder aux documents émanant d'un organisme public.

L'AMP est assujettie à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (« Loi sur l'accès »), qui prévoit les modalités de ce droit d'accès.

Elle doit également se conformer aux obligations prévues au *Règlement sur la diffusion de l'information et la protection des renseignements personnels*, qui rend obligatoire la diffusion systématique de certaines informations afin de favoriser la transparence des organismes publics.

Conséquemment, l'AMP publie sur son site Internet les décisions anonymisées des demandes d'accès lui ayant été adressées et les documents transmis. Elle diffuse également certains renseignements relatifs à l'organisation, dont les codes d'éthique des employés et membres de la haute direction, des informations relatives aux dépenses de l'organisation et des renseignements relatifs à la rémunération et aux avantages de membres de la haute direction.

L'AMP doit faciliter l'exercice du droit d'accès à l'information et prévoir des mesures d'accompagnement pour une personne exerçant ce droit.

Le respect du plan de classification en vigueur rend possible le repérage des documents faisant l'objet d'une demande d'accès à l'information. Le traitement des demandes est fait de façon objective, en respectant l'encadrement légal et les exceptions applicables.

L'information accessible est divulguée de manière transparente. Le droit d'accès aux documents de l'AMP n'est restreint que dans les cas d'exceptions prévus expressément à la Loi sur l'accès.

18. DÉLAIS DE TRAITEMENT D'UNE DEMANDE D'ACCÈS À L'INFORMATION

Le traitement d'une demande d'accès à l'information doit se faire dans les délais impartis par la Loi sur l'accès.

Le responsable de l'accès à l'information doit répondre au requérant au plus tard dans les 20 jours qui suivent la date de réception d'une telle demande. Lorsqu'il est impossible de donner suite à la demande dans ce délai, le délai peut être prolongé pour une période n'excédant pas dix jours en donnant avis au requérant.

Le repérage rapide, complet et sérieux des documents faisant l'objet de la demande d'accès à l'information est primordial afin de se conformer aux dispositions législatives.

19. CONTESTATION D'UNE DÉCISION RENDUE

Une personne qui souhaite contester une décision rendue par le responsable de l'accès à l'information de l'AMP doit adresser une demande de révision à la Commission d'accès à l'information (CAI).

20. RÔLES ET RESPONSABILITÉS

20.1 Dirigeant de l'organisme public

Le président-directeur général de l'AMP doit veiller à assurer le respect et la mise en œuvre de la Loi sur l'accès.

Il peut déléguer la fonction de responsable de l'accès aux documents à un membre du personnel-cadre, mais il demeure imputable à titre de plus haut dirigeant.

À l'AMP, cette fonction est déléguée au secrétaire général.

20.2 Responsable de l'accès à l'information et de la protection des renseignements personnels

Le secrétaire général est responsable de l'accès à l'information et de la protection des renseignements personnels.

En tant que responsable de l'accès à l'information, il doit :

- Veiller au respect de la Loi sur l'accès;
- Recevoir et traiter les demandes d'accès à l'information adressées à l'AMP;
  - Il peut s'adjoindre la collaboration d'une avocate ou d'un avocat au Secrétariat général afin de traiter les demandes reçues.
- Statuer sur l'admissibilité des documents demandés;
- Rendre les décisions relatives aux demandes d'accès à l'information dans les délais prescrits par la Loi sur l'accès;
- Collaborer avec la Direction des affaires juridiques et du contentieux pour fournir les renseignements pertinents au dossier lors de la contestation d'une décision rendue à la Commission d'accès à l'information.

Le responsable de l'accès à l'information est membre d'office du comité sur la protection de l'information.

20.3 Secrétariat général

Le Secrétariat général est responsable du suivi des obligations législatives et réglementaires en matière d'accès à l'information.

20.4 Direction des affaires juridiques et du contentieux

La Direction des affaires juridiques et du contentieux est impliquée lorsqu'il y a contestation à la CAI d'une décision rendue par le responsable de l'accès à l'information.

Une avocate ou un avocat est responsable de la prise en charge du dossier litigieux et représente l'AMP devant la CAI.

20.5 Gestionnaires

Chaque gestionnaire est responsable de promouvoir et de faire appliquer les principes d'accès à l'information au sein de sa direction ou son service.

De plus, le gestionnaire doit :

- Collaborer avec le responsable de l'accès à l'information et de la protection des renseignements personnels lors de la réception d'une demande auprès de sa direction ou son service;
- Transmettre intégralement les documents demandés au responsable de l'accès à l'information ou désigner une personne de sa direction ou son service pour ce faire.

20.6 Membre du personnel

Chaque membre du personnel est responsable d'enregistrer et de classer adéquatement les documents produits dans le cadre de son travail afin de les rendre accessibles.

Il doit prendre connaissance et respecter les encadrements en vigueur.

PROTECTION DES RENSEIGNEMENTS PERSONNELS

21. CONTEXTE

La protection des renseignements personnels est considérée comme l'une des composantes du droit à la vie privée, prévu à la Charte des droits et libertés de la personne ainsi qu'au Code civil du Québec.

À l'AMP, la protection des renseignements personnels est encadrée par la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*. Cette loi exige qu'un organisme public s'assure du respect de la confidentialité des renseignements qu'il détient concernant une personne, durant tout leur cycle de vie.

L'AMP a l'obligation de protéger les renseignements personnels contre l'accès, l'utilisation ou la communication non autorisés par la loi de même que contre l'atteinte ou la perte de ces renseignements. Toute personne physique doit aussi pouvoir accéder aux renseignements personnels que l'organisme détient sur elle et pouvoir demander la rectification de ceux-ci en cas d'inexactitude.

Dans le cadre de ses activités et de sa mission, l'organisation reçoit et traite de nombreux renseignements personnels et confidentiels. L'AMP est responsable des renseignements personnels qu'elle détient. Par conséquent, elle doit prendre toutes les mesures nécessaires afin d'en assurer leur protection.

Elle est également tenue de respecter des obligations en matière de gestion, de traitement des incidents de confidentialité, de communication de renseignements personnels et d'évaluation des facteurs relatifs à la vie privée.

22. PLAN D'ACTION ET FORMATION DU PERSONNEL

Afin de respecter les obligations qui lui incombent en matière de protection des renseignements personnels, l'AMP met en œuvre un plan d'action portant sur la protection des renseignements personnels, qui vient appuyer le développement d'une culture organisationnelle axée sur le respect du droit à la vie privée.

Le Secrétariat général élabore, en collaboration avec la Direction des technologies de l'information, un plan annuel de sensibilisation du personnel qui vise à promouvoir les bonnes pratiques de gestion de l'information et la protection des renseignements personnels. Les activités de sensibilisation comprennent la diffusion de capsules d'information, la publication d'articles et la réalisation d'activités ponctuelles dans les bureaux de l'AMP.

L'AMP mise sur la formation de son personnel pour renforcer la protection des renseignements personnels. Chaque employé doit suivre une formation obligatoire d'introduction à la protection des renseignements personnels qui est dispensée par un avocat du Secrétariat général. Un plan de formation en continu sera mis en place pour permettre à l'ensemble des employés de l'organisation de parfaire et mettre à jour leurs connaissances sur les différents volets de la protection des renseignements personnel.

23. COMMUNICATION DE RENSEIGNEMENTS PERSONNELS

La communication de renseignements personnels détenus par l'AMP peut se faire avec l'obtention du consentement de la personne qu'ils concernent. Ce consentement doit être manifeste, libre, éclairé, donné à des fins spécifiques et limité dans le temps.

Les renseignements personnels ne peuvent être communiqués sans le consentement de la personne concernée, sauf dans les cas d'exception expressément prévus par la Loi sur l'accès.

L'AMP a l'obligation de tenir un registre pour les situations suivantes :

- Communication d'un renseignement personnel
- Entente de collecte de renseignements personnels
- Renseignement personnel utilisé à une fin autre que celle pour laquelle il a été recueilli

Ces registres ont un caractère public.

Le responsable de l'accès à l'information et de la protection des renseignements personnels ou une avocate ou un avocat au Secrétariat général désigné par celui-ci à cette fin tient les registres et les met à jour.

24. RÉALISATION DE SONDAGES

Avant de réaliser un sondage qui implique la collecte ou la communication de renseignements personnels, le gestionnaire de l'unité d'affaires qui désire réaliser le sondage doit consulter le conseiller stratégique en protection des renseignements personnels. Ensemble, ils doivent:

- Déterminer la nécessité de recourir au sondage;
- Évaluer l'aspect éthique du sondage, compte tenu notamment de :
    - ◇ La quantité et le type de renseignements concernés
    - ◇ La sensibilité des renseignements communiqués ou recueillis
    - ◇ La finalité de leur utilisation
- Vérifier si le consentement des personnes est requis pour réaliser le sondage;
- Établir les modalités du sondage ainsi que les renseignements à communiquer aux personnes sollicitées
- Déterminer si l'utilisation des renseignements recueillis doit faire l'objet d'une inscription dans un registre prévu par la Loi sur l'accès
- Déterminer toute mesure nécessaire pour assurer la conformité du sondage à la Loi sur l'accès

En tout temps, l'AMP doit s'assurer que les personnes, tant à l'interne qu'à l'externe, se sentent libres de répondre ou non aux questions d'un sondage réalisé. Il est strictement prohibé de contraindre une personne à répondre à une question posée dans le cadre d'un sondage ou d'exercer quelconque mesure de représailles contre une personne qui refuse d'y répondre.

25. INCIDENTS DE CONFIDENTIALITÉ

25.1 Types d'incident de confidentialité

Un incident de confidentialité peut résulter de l'une ou l'autre des situations suivantes :

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

25.2 Registre des incidents

L'AMP doit obligatoirement tenir un registre des incidents de confidentialité.

Elle doit y consigner les renseignements suivants :

- Description des renseignements personnels visés par l'incident;
- Description des circonstances de l'incident;
- Date ou période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de la période;
- Date ou période au cours desquelles l'organisation a pris connaissance de l'incident;
- Nombre de personnes concernées par l'incident;
- Description des éléments qui amènent l'organisation à conclure qu'il existe ou non un risque qu'un préjudice sérieux soit causé aux personnes concernées;

- Si l'incident présente un risque de préjudice sérieux, les dates de transmissions des avis à la Commission d'accès à l'information et aux personnes concernées;
- Description des mesures prises par l'organisation afin de diminuer les risques qu'un préjudice soit causé.

Ce registre permet de répertorier les incidents et de mieux identifier les risques présents au sein de l'AMP, afin de mettre en place des mesures permettant de limiter au maximum les risques de survenance de tels incidents.

25.3 Évaluation du niveau de risque de préjudice d'un incident de confidentialité

Chaque incident de confidentialité doit faire l'objet d'une évaluation de son niveau de risque de préjudice.

La méthode d'évaluation du niveau de risque est établie par le Secrétariat général.

En cas d'incident de confidentialité, cette évaluation est réalisée par le responsable de l'accès à l'information et de la protection des renseignements personnels, qui peut requérir la participation de toute autre personne désignée.

25.4 Avis aux personnes concernées

Les personnes concernées par l'incident de confidentialité sont avisées par l'AMP par écrit, au moyen d'une lettre signée par le responsable de l'accès à l'information et de la protection des renseignements personnels.

L'avis contient les renseignements suivants :

- Description sommaire de l'incident;
- Type(s) de renseignements personnels ayant fait l'objet de l'incident;
- Mesures prises par l'AMP pour mitiger les conséquences;
- Mesures correctives mises en place à l'AMP pour diminuer les risques qu'un tel incident se reproduise.

25.5 Avis à la Commission d'accès à l'information

Un avis écrit est envoyé à la Commission d'accès à l'information, par le responsable de l'accès à l'information et de la protection des renseignements personnels, pour tout incident de confidentialité qui présente un risque sérieux qu'un préjudice soit causé.

L'AMP peut procéder à la divulgation volontaire à la CAI d'un incident de confidentialité, même si l'événement ne présente pas de risque sérieux de préjudice.

26. ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE

L'évaluation des facteurs relatifs à la vie privée (ÉFVP) est un processus de gestion de risques qui permet de déterminer l'incidence éventuelle d'un projet, d'une activité ou d'un programme sur la vie privée et la protection des renseignements personnels. Elle permet aussi d'évaluer le respect aux exigences légales et principes fondamentaux en protection des renseignements personnels.

La démarche consiste à évaluer tous les facteurs qui auront un impact positif ou négatif pour le respect de la vie privée des personnes concernées et d'établir, au terme de cette évaluation, les mesures permettant de mieux protéger leurs renseignements personnels et de réduire les risques à un niveau acceptable.

L'intégration volontaire de l'ÉFVP dès les premières phases de la gestion d'un projet, d'une activité ou d'un programme est une bonne pratique qui favorise l'application de la confidentialité par défaut.

À compter du mois de septembre 2023, l'AMP devra obligatoirement réaliser une ÉFVP dans les cas suivants:

- Tout projet d'acquisition de développement et de refonte de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels;
- Toute communication de renseignements personnels sans le consentement de la personne concernée, dans les cas prévus par la loi;

- La collecte de renseignements personnels pour un autre organisme public, avant la conclusion de l'entente et sa transmission à la CAI;
- La communication de renseignements personnels à l'extérieur du Québec.

27. RÔLES ET RESPONSABILITÉS

27.1 Dirigeant de l'organisme public

Le président-directeur général de l'AMP est imputable de la protection des renseignements personnels au sein de l'organisation.

Il peut déléguer la fonction de responsable la protection des renseignements personnels à un membre du personnel, mais il en demeure le premier responsable.

Cette fonction est déléguée au secrétaire général, qui exerce ce rôle de manière concomitante avec son rôle de responsable de l'accès à l'information.

27.2 Responsable de l'accès à l'information et de la protection des renseignements personnels

Le secrétaire général est responsable de l'accès à l'information et de la protection des renseignements personnels.

En tant que responsable de la protection des renseignements personnels, il doit :

- Veiller au respect de la Loi sur l'accès et à la mise en œuvre des mesures de protection des renseignements personnels au sein de l'AMP;
- Procéder à l'évaluation du risque de préjudice lors de la survenance d'un incident de confidentialité, afin de déterminer les actions à mettre en œuvre en matière de protection des renseignements personnels.
- Aviser par écrit les personnes concernées par un incident de confidentialité;
- Aviser la CAI de tout incident de confidentialité qui survient à l'AMP et qui présente un risque de préjudice.

27.3 Conseiller stratégique en protection des renseignements personnels

Le conseiller stratégique en protection des renseignements personnels est l'avocate ou l'avocat du Secrétariat général qui assure un rôle-conseil et un soutien juridique pour les questions relatives à la protection des renseignements personnels et confidentiels auprès de l'ensemble du personnel de l'AMP.

Cette personne est responsable du déploiement et de la mise en œuvre du plan d'action en protection des renseignements personnels.

27.4 Secrétariat général

Le Secrétariat général est responsable du suivi des obligations législatives et réglementaires en matière de protection des renseignements personnels.

27.5 Responsable de la gestion documentaire

La responsable de la gestion documentaire s'assure de la gestion de l'ensemble des documents de l'AMP, tout au long de leur cycle de vie. Elle s'assure que le stockage et la destruction des renseignements personnels contenus dans ces documents se font conformément au calendrier de conservation approuvé et au cadre législatif applicable.

27.6 Chef organisationnel de la sécurité de l'information

Le chef organisationnel de la sécurité de l'information (CSIO) est un répondant désigné en sécurité de l'information à l'AMP.

Il doit :

- Considérer la protection des renseignements personnels dans l'application et la mise en œuvre de mesures de sécurité de l'information à l'AMP;
- Assurer le lien vers le Secrétariat général pour transmettre l'information concernant les enjeux de protection des renseignements personnels;

- Aviser le responsable de l'accès à l'information et de la protection des renseignements personnels de tout incident de sécurité impliquant un incident de confidentialité, afin que les démarches relatives aux exigences en protection des renseignements personnels soient appliquées dans les plus brefs délais.

27.7 Coordonnateur organisationnel des mesures de sécurité de l'information

Le coordonnateur organisationnel des mesures de sécurité de l'information (COMSI) est responsable de l'opérationnalisation des mesures de sécurité informatique visant à protéger les actifs informationnels de l'AMP à l'interne, qui inclut la protection des renseignements personnels détenus par l'organisation.

Le COMSI doit également coordonner les mesures de sécurité gérées à l'externe par le ministère de la Cybersécurité et du numérique.

27.8 Gestionnaires

Chaque gestionnaire est responsable de promouvoir et faire appliquer les principes de protection des renseignements personnels au sein de sa direction ou son service.

De plus, le gestionnaire doit :

- Collaborer avec le responsable de l'accès à l'information et de la protection des renseignements personnels lors de la réception d'une demande auprès de sa direction ou son service, afin de fournir les documents demandés;
- Aviser le responsable de l'accès à l'information et de la protection des renseignements personnels lorsqu'une situation portée à sa connaissance engendre un risque relatif à la protection des renseignements personnels détenus par l'AMP.

27.9 Membre du personnel

Chaque membre du personnel a la responsabilité de veiller à la protection des renseignements personnels et confidentiels qu'il produit, utilise et reçoit dans le cadre de son travail.

Il doit prendre connaissance des encadrements en vigueur et appliquer les mesures mises en place par l'AMP

SÉCURITÉ DE L'INFORMATION

28. CONTEXTE

L'AMP est assujettie à la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*, aux règlements qui en découlent, ainsi qu'aux règles et orientations gouvernementales en sécurité de l'information.

La *Directive gouvernementale sur la sécurité de l'information* prévoit qu'un organisme public a la responsabilité d'assurer la sécurité des ressources informationnelles et de l'information qu'il détient ou utilise, même lorsque la conservation de celles-ci est assurée par un tiers.

La sécurité de l'information consiste en un ensemble de mesures appliquées et d'outils déployés pour assurer la protection des informations et des données détenues par l'organisation, tout au long de leur cycle de vie. Elle permet d'assurer la continuité des activités de l'AMP et de maintenir la confiance du public à l'égard de l'organisation.

La sécurité de l'information se décline en plusieurs composantes, dont :

- La sécurité informatique
- La protection des renseignements personnels
- L'accès aux documents
- La mise en place d'encadrements

À l'AMP, l'information est catégorisée afin de déterminer son niveau de protection adéquat eu égard aux risques encourus en fonction de sa disponibilité, de son intégrité et de sa confidentialité (cote DIC).

29. STRUCTURE GOUVERNEMENTALE DE SÉCURITÉ DE L'INFORMATION

En matière de sécurité de l'information, les rôles ont été répartis sur trois niveaux :

- Gouvernemental
- Portefeuille
- Organisationnel

Cette structure vise à assurer une cohérence et une coordination des interventions réalisées.

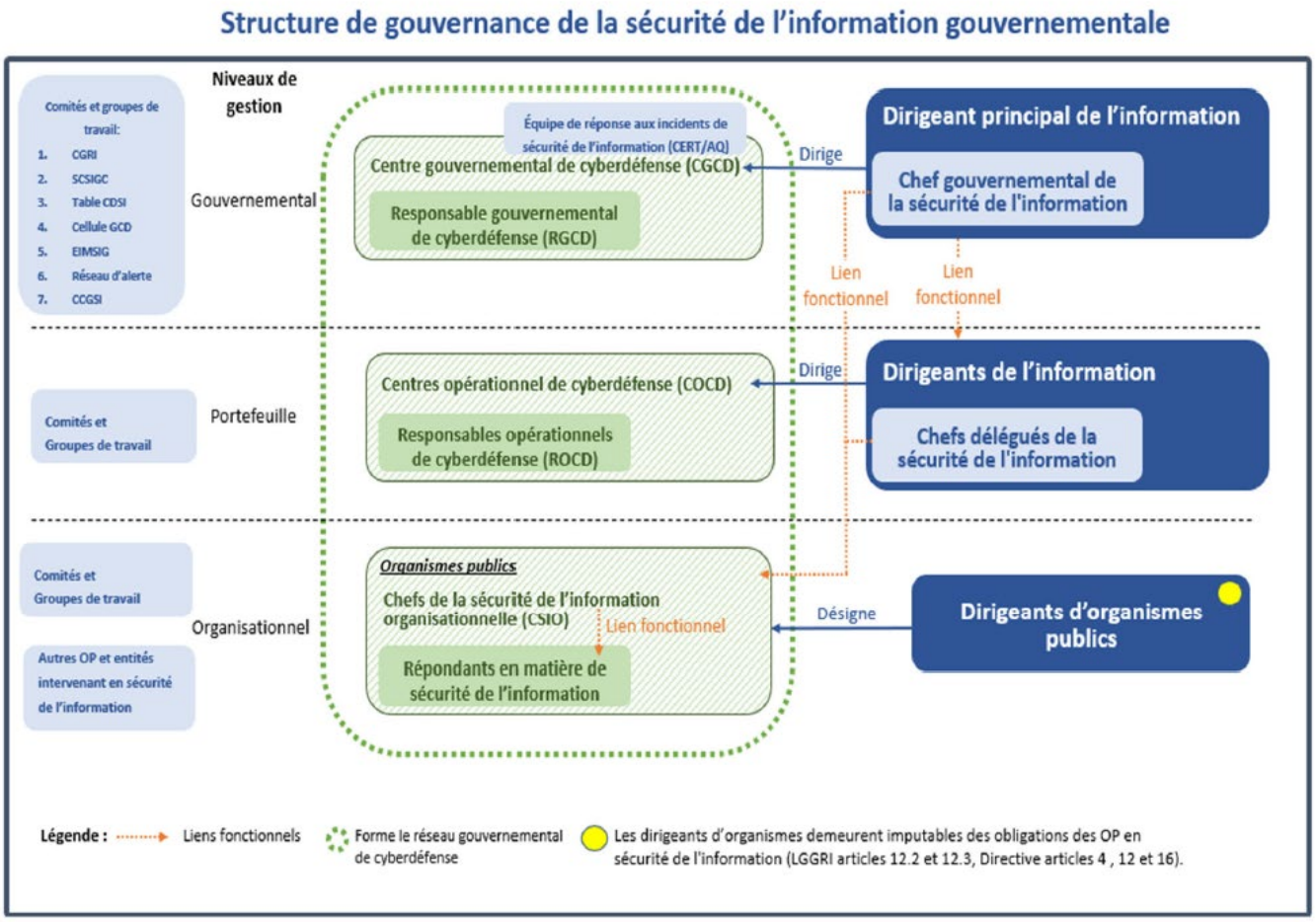
29.1 Ministère de la cybersécurité et du numérique

Le ministère de la Cybersécurité et du numérique (MCN) joue un rôle central de soutien en sécurité de l'information pour les organismes publics et les ministères.

Il détient tous les pouvoirs pour soutenir les organismes, ce qui inclut notamment de pouvoir conclure des ententes avec toute personne, organisme canadien ou étranger pour assurer la sécurité de l'information. Il établit les mécanismes de contrôle et procède à des audits pour s'assurer de l'atteinte des objectifs.

29.2 Réseau gouvernemental de cyberdéfense

Le réseau gouvernemental de cyberdéfense est formé des responsables en sécurité de l'information désignés à chacun des niveaux, qui forment des instances de concertation distinctes.



Source : Cadre gouvernemental de gestion de la sécurité de l'information

Le processus de gestion des incidents, vulnérabilités et incidents élaboré par le MCN détermine le niveau de réponse, ainsi que les rôles et les responsabilités des intervenants du Centre gouvernemental de cyberdéfense en fonction du niveau d'impact du préjudice envers le citoyen.

Ce niveau d'impact est mesuré en fonction des critères suivants :

- Type de préjudice
- Probabilité de concrétisation
- Urgence d'agir

30. REGISTRE DES ÉVÉNEMENTS DE SÉCURITÉ

L'AMP tient un registre des événements de sécurité, conformément aux dispositions prévues dans la Directive gouvernementale sur la sécurité de l'information, qui contient les renseignements suivants :

- Coordonnées du CSIO
- Date et heure de l'événement
- Localisation de l'événement
- Nature de l'événement
- Description de l'événement
- Préjudices engendrés et personnes morales ou physiques concernées
- Actions prises
- Acceptation ou non du risque résiduel et justification
- Actions prévues
- Date de clôture de l'événement

Ce registre permet de consigner l'information nécessaire à la gestion des risques reliés aux menaces, vulnérabilités et incidents en sécurité de l'information.

31. RÔLES ET RESPONSABILITÉS

31.1 Dirigeant de l'organisme public

Le président-directeur général de l'AMP est responsable de la sécurité de l'information relevant de son autorité. Il s'assure du respect des lois et des bonnes pratiques établies dans l'organisation en matière de sécurité de l'information.

Il désigne les personnes responsables de la sécurité de l'information au sein de l'AMP.

31.2 Chef de la sécurité de l'information organisationnelle

Le chef de la sécurité de l'information organisationnelle (CSIO) assure la responsabilité de la prise en charge globale de la sécurité de l'information au sein de l'AMP.

À ce titre, il doit:

- Apporter au président-directeur général le soutien nécessaire lui permettant d'assumer ses obligations en sécurité de l'information;
- Agir en tant que porte-parole du dirigeant principal de l'information (DPI) du gouvernement auprès de l'AMP;
- Relayer les orientations et priorités d'intervention gouvernementales en sécurité de l'information à l'AMP;
- Assurer un lien fonctionnel entre l'AMP et les entités gouvernementales impliquées en sécurité de l'information;
- Aviser le chef délégué de la sécurité de l'information auquel l'AMP est rattachée lorsqu'un événement de sécurité présente un risque de préjudice sérieux.

31.3 Coordonnateur des mesures de sécurité de l'information

Le coordonnateur des mesures de sécurité de l'information (COMSI) est un répondant spécifique désigné à l'AMP pour coordonner les mesures à prendre en sécurité de l'information, conformément au Processus de gestion des menaces, vulnérabilités et incidents (GMVI) élaboré par le MCN.

Il a la responsabilité de :

- Représenter l'AMP et participer activement au Réseau d'alerte gouvernemental coordonné par l'Équipe de réponse aux incidents de sécurité de l'information de l'Administration québécoise (CERT/AQ);
- Procéder à l'identification des menaces, vulnérabilités et incidents touchant l'AMP et en tenir le CSIO informé;
- S'assurer de l'élaboration, la mise à jour et l'application d'un plan interne de réponse aux menaces, vulnérabilités et incidents;
- S'assurer de la réalisation d'analyses de risques de sécurité;
- Collaborer avec le CSIO de l'AMP et le responsable opérationnel de cyberdéfense (ROCD) du Secrétariat du Conseil du trésor en leur assurant notamment le soutien technique nécessaire à l'exercice de leurs responsabilités.

31.4 Vice-présidence à l'administration

La Vice-présidence à l'administration, plus précisément l'équipe dédiée aux ressources informationnelles, collabore avec les autres rôles en gestion afin d'assurer l'implantation des mesures de sécurité de l'information. Elle doit :

- Assurer un lien fonctionnel entre l'AMP et le MCN pour l'application de l'entente qui unit les deux organisations;
- Catégoriser l'information détenue par l'AMP (cote DIC);
- Signaler les menaces, les vulnérabilités et les incidents au COMSI;
- Tenir et mettre à jour le registre des incidents de sécurité;
- Informer le personnel de tout événement en sécurité de l'information qui nécessite une vigilance accrue des utilisatrices et des utilisateurs ou des mesures à prendre avec les équipements informatiques;
- Informer le responsable de l'accès à l'information et de la protection des renseignements personnels lors de la survenance d'un incident de sécurité impliquant un incident de confidentialité.

Le chef de la sécurité de l'information organisationnelle est membre d'office du comité sur la protection de l'information.

31.5 Secrétariat général

Le Secrétariat général assure un rôle-conseil et un soutien juridique en matière de gestion et gouvernance auprès des responsables de la sécurité de l'information à l'AMP.

En cas d'incident de sécurité impliquant un incident de confidentialité, le Secrétariat général est responsable d'appliquer les mesures relatives à la protection des renseignements personnels.

31.6 Gestionnaires

Chaque gestionnaire est responsable de promouvoir et faire appliquer les mesures en sécurité de l'information au sein de sa direction ou son service.

31.7 Membre du personnel

Chaque membre du personnel a la responsabilité de suivre les bonnes pratiques organisationnelles établies par l'AMP en sécurité de l'information. Le personnel doit également :

- Signaler tout incident de sécurité de l'information potentiel ou avéré;
- Prendre connaissance et appliquer les mesures de sécurité de l'information mises en place par l'AMP.