Commission
d'accès à l'information
du Québec

# Procédure de gestion des incidents de confidentialité

2023-07-24

# Table des matières

## 1. Contexte

En cas d'incident de confidentialité, la Commission d'accès à l'information (CAI) doit intervenir afin de minimiser les risques de préjudice envers les personnes concernées et d'éviter de nouveaux incidents de même nature. Elle doit aussi tenir un registre de ces incidents. Les annexes suivantes soutiennent l'application de la *Procédure de gestion des incidents de confidentialité* (ci-après la « Procédure ») : une fiche d'incident de confidentialité, une grille d'évaluation du risque de préjudice sérieux, un modèle d'avis pour les personnes concernées et susceptibles de subir un risque de préjudice sérieux, un registre de communications des renseignements en lien avec des incidents de confidentialité, une liste des personnes répondantes pouvant prêter assistance, un registre des incidents de confidentialité et un modèle d'avis public qui sera soumis pour approbation auprès du Comité de l'accès à l'information et à la protection des renseignements personnels (AIPRP).

## 2. Champ d'application

La Procédure décrit et encadre la démarche à suivre lorsqu'il y a motif de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel détenu par la CAI. Elle rappelle l'obligation de signalement, prévoit les étapes de traitement de l'incident de confidentialité et définit les rôles et responsabilités des parties prenantes.

Les membres de la CAI et son personnel, y compris les étudiants, les stagiaires et les contractuels, sont tenus de se conformer à la présente Procédure.

## 3. Collaboration

La responsabilité de la gestion des incidents de confidentialité est attribuée au responsable de l'accès aux documents et de la protection des renseignements personnels de la CAI (ci-après le « responsable de l'accès »). Le responsable est appuyé dans cette responsabilité par le Comité AIPRP. De plus, la collaboration de tout le personnel est attendue, à la demande du responsable de l'accès.

Les étapes de la Procédure peuvent aussi être réalisées simultanément, selon les circonstances.

## 4. Encadrement légal, réglementaire et administratif

L'application de la Procédure est encadrée par :

1. La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1, art. 63.8 à 63.11);
2. Le *Règlement sur les incidents de confidentialité*.

## 5. Définitions

Incident en sécurité de l'information : événement pour lequel il y a un risque d'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information gouvernementale. Un incident n'est pas obligatoirement lié à l'utilisation des technologies de l'information.

Incident de confidentialité : accès, utilisation ou communication non autorisée par la loi d'un renseignement personnel, de même que la perte d'un renseignement personnel ou toute autre atteinte à sa protection.

Personne concernée : personne physique dont les renseignements personnels sont exposés à un risque en raison de la survenance d'un incident de confidentialité.

Préjudice sérieux : acte ou événement susceptible de porter atteinte à la personne concernée ou à ses biens et de nuire à ses intérêts de manière non négligeable.

Renseignement personnel : renseignement portant sur une personne physique et permettant de l'identifier directement ou indirectement. Il est confidentiel et ne peut être communiqué sans le consentement de la personne concernée, sauf exception.

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

# 6. Étapes de l'intervention en cas d'incident

## 6.1 Signalement de l'incident de confidentialité

Dès qu'un membre du personnel de la CAI a un motif de croire que s'est produit un incident de confidentialité, il doit aviser sans délai son supérieur immédiat. S'il s'agit d'un incident de confidentialité, le supérieur immédiat doit en aviser sans délai le responsable de l'accès et de la protection des renseignements personnels de la CAI :

Jorge Passalacqua

Par téléphone : 514 873-4196, poste 52601, ou 514 502-6631

Par courriel : jorge.passalacqua@cai.gouv.qc.ca

En cas d'absence du responsable de l'accès, le supérieur immédiat communique avec la substitute du responsable de l'accès :

Catherine-Isabelle Valois

Par téléphone : 514 873-4196, poste 52602

Par courriel : catherine-isabelle.valois@cai.gouv.qc.ca

Dans le cas où le supérieur immédiat est absent ou ne peut être joint rapidement, la personne qui a constaté l'incident communique directement avec le responsable de l'accès.

Le responsable de l'accès ou sa substitute avise le chef de la sécurité de l'information organisationnelle (CSIO) :

Rémi Bédard

Par téléphone : 418 953-1044, poste 51401

Par courriel : remi.bedard@cai.gouv.qc.ca

Le responsable de l'accès ou sa substitute peut constituer un groupe de travail afin de lui porter assistance dans la gestion de l'incident. Une liste des personnes qui peuvent collaborer et prêter assistance se trouve à l'annexe 8. Au besoin, ces personnes peuvent déléguer des membres du personnel de leur unité administrative pour collaborer au sein du groupe de travail.

## 6.2 Détermination de la situation

Le responsable de l'accès, en collaboration avec toute personne dont le soutien est nécessaire, selon les circonstances, doit déterminer et documenter les circonstances objectives de l'incident de confidentialité. Dans le cadre de cette démarche, il doit, notamment :

1. Établir le moment et l'endroit où l'incident s'est produit (date ou période où l'incident a eu lieu, endroit physique, etc.);

2. Identifier les personnes dont les renseignements personnels sont concernés;

3. Identifier les renseignements personnels impliqués et leur nature;

4. Identifier les membres du personnel impliqués et leur rôle;

5. Identifier les systèmes ou processus en cause;

6. Trouver la cause de l'incident (erreur, vulnérabilité, faille, rançongiciel, cyberattaque, vol, accès non autorisé, etc.).

Cette démarche de détermination des circonstances doit se poursuivre tant que tous les éléments pertinents sur l'incident n'ont pas été clairement identifiés. Le responsable de l'accès doit s'assurer de documenter sa démarche en remplissant une fiche d'incident (annexe 1). Il peut exiger un compte rendu (annexe 1) de l'unité administrative où s'est produit l'incident, ou de la personne ayant découvert l'incident, le cas échéant.

### 6.3 Évaluation du préjudice

Le responsable de l'accès, en collaboration avec toute personne dont le soutien est nécessaire, selon les circonstances, doit évaluer le niveau du préjudice susceptible d'être causé aux personnes dont les renseignements personnels sont concernés par l'incident.

Le responsable de l'accès doit compléter la grille d'évaluation du risque de préjudice sérieux (annexe 2). Cette grille permet d'évaluer les risques de préjudice pour tout incident ayant lieu au sein de l'organisation. Le préjudice sérieux n'a pas à s'être matérialisé : il doit seulement être susceptible de se produire. Selon le résultat de l'évaluation, le responsable de l'accès détermine s'il y a absence ou présence d'un préjudice sérieux.

Le responsable de l'accès s'assure que tout incident est consigné dans le registre des incidents de confidentialité (annexe 7).

En la présence d'un risque de préjudice sérieux, il doit :

- Aviser la Direction de la surveillance et lui transmettre le formulaire d'avis complété (annexe 3 ou version plus récente diffusée sur le site Web de la CAI);
- Aviser toute personne concernée susceptible de subir un risque de préjudice sérieux (annexe 4);
- Aviser toute personne ou organisme susceptible d'atténuer le risque;

- Consigner le risque dans le registre des incidents de confidentialité (annexe 7);
- Consigner l'incident dans le registre des communications, le cas échéant (annexe 6).

L'ordre dans lequel ces actions sont réalisées peut varier selon les circonstances.

### 6.4 Atténuation du risque

Peu importe si le risque de préjudice est sérieux ou non, le responsable de l'accès, en collaboration avec toute personne dont l'intervention est jugée nécessaire, doit prendre rapidement les mesures raisonnables requises afin d'atténuer les risques de préjudice. Il doit également prendre les mesures nécessaires pour éviter que de nouveaux incidents de la même nature se reproduisent. Ces actions peuvent être réalisées en collaboration avec toute personne dont le soutien peut être utile, selon les circonstances.

Le responsable de l'accès informe le Comité AIPRP dans les meilleurs délais et tient compte de ses recommandations visant une gestion adéquate de l'incident.

Entre autres, le responsable de l'accès doit :

1. S'assurer que la pratique ou le processus à l'origine de l'incident a cessé ou a été corrigé;

2. S'assurer que les renseignements personnels impliqués sont récupérés ou détruits;

3. Réaliser des vérifications ultérieures sur les mesures mises en place pour s'assurer que le niveau de protection des renseignements personnels est adéquat, et toute action jugée pertinente dans les circonstances. Par exemple, le responsable de l'accès doit s'assurer que les mots de passe et les codes d'accès informatiques sont modifiés, au besoin. Il doit aussi s'assurer que les codes d'accès aux locaux et l'attribution des clés sont adaptés et, en collaboration avec le Chef organisationnel de la sécurité de l'information, que les lacunes informatiques sont corrigées;

4. S'assurer que le personnel et les membres de la CAI sont sensibilisés et formés pour réduire les risques d'erreur humaine dans la gestion des renseignements personnels;

5. Prendre tout autre mesure appropriée selon le type d'incident.

### 6.5 Avis à la Commission d'accès à l'information (Direction de la surveillance)

Lorsqu'il est déterminé qu'un incident présente un risque de préjudice sérieux, le responsable de l'accès doit aviser la Direction de la surveillance de la CAI, avec diligence et par écrit, en lui transmettant le formulaire d'avis complété (annexe 3 ou version plus récente diffusée sur le site Web de la CAI). Toute information complémentaire touchant des éléments que doit contenir l'avis et dont l'organisation prend connaissance suivant l'envoi de cet avis doit être transmise, avec diligence, dès le moment où elle est recueillie.

### 6.6 Avis aux personnes concernées et à toute personne ou à tout organisme susceptible d'atténuer le risque

Lorsqu'il est déterminé qu'un incident présente un risque de préjudice sérieux, le responsable de l'accès doit aviser toute personne dont un renseignement personnel est concerné par l'incident. L'avis (annexe 4) peut être fait soit par courriel ou par lettre postale. Toutefois, la personne concernée n'a pas à être avisée si cela est susceptible d'entraver une enquête menée par une personne ou un organisme qui, en vertu de la loi, est chargé de prévenir, de détecter ou de réprimer le crime ou les infractions aux lois.

Dans le cas où il est déterminé que l'avis est nécessaire, il doit minimalement contenir les informations suivantes :

1. Les coordonnées complètes de la personne concernée par l'incident;
2. Le rôle de la personne concernée par l'incident (ex. citoyen, personnel de la CAI, fournisseur, etc.);
3. Le(s) numéro(s) de dossier(s), le cas échéant;
4. Une brève description des circonstances de l'incident (date et lieu);
5. Les renseignements personnels concernés par l'incident (si l'information n'est pas connue, fournir la raison justifiant l'impossibilité de fournir la description);
6. Une brève description des mesures prises par la Commission et autres parties pour atténuer les risques de préjudice sérieux;
7. Des suggestions de mesures permettant d'atténuer le risque de préjudice sérieux à la personne concernée;
8. Les coordonnées du responsable de l'accès afin que la personne concernée puisse se renseigner davantage sur l'incident.

Si la personne visée n'est pas joignable ou si ses coordonnées sont inconnues, le responsable de l'accès peut recourir à un avis public afin que la personne concernée puisse indirectement prendre connaissance de l'incident, tout en s'assurant qu'il s'agit également d'un moyen de réduire les risques.

Le responsable de l'accès pourrait considérer, après avoir consulté le Comité AIPRP, qu'il est pertinent et opportun d'aviser d'autres intervenants susceptibles d'atténuer le risque de préjudice sérieux. À cette fin, seuls les renseignements personnels nécessaires à l'atteinte de cet objectif sont transmis. Le consentement de la personne concernée par les renseignements transmis n'est pas requis. Le responsable de l'accès doit documenter la démarche en inscrivant dans le registre des communications (annexe 6) :

1. Le numéro de(s) dossier(s), le cas échéant;
2. Le moment de la communication des renseignements;
3. Le ou les destinataires des renseignements;
4. Les circonstances de la communication des renseignements;
5. Les renseignements transmis;
6. Les objectifs poursuivis.

### 6.7 Inscription de l'incident au registre des incidents de confidentialité

Le registre des incidents de confidentialité (annexe 7) est rempli par le responsable de l'accès. Le registre permet de documenter tous les incidents de confidentialité concernant des renseignements personnels détenus par la Commission ou pour son compte, qu'il y ait un risque de préjudice sérieux ou non.

Le registre doit contenir les renseignements suivants :

1. Le(s) numéro(s) de dossier(s);
2. La date ou la période où l'incident est survenu ou une approximation de la période, le cas échéant;
3. La date de prise de connaissance de l'incident;
4. La date de la transmission de l'avis de l'incident au responsable de la protection des renseignements personnels;
5. La date de la transmission de l'avis à la Commission;
6. Une description des renseignements personnels concernés par l'incident;

7. Une brève description des circonstances de l'incident;

8. Le nombre de personnes concernées par l'incident ou une approximation du nombre de personnes, le cas échéant;

9. Une description des éléments portant à croire qu'il existe ou non un risque de préjudice sérieux;

10. La date de la transmission d'un avis aux personnes concernées, si l'incident présente un risque de préjudice sérieux, ou la date de la transmission d'un avis public, le cas échéant;

11. La date de la transmission d'un avis à toute personne ou à tout organisme susceptible d'atténuer le risque;

12. Les mesures prises pour remédier, atténuer ou contenir les conséquences négatives de l'incident et celles visant à prévenir d'autres incidents de même nature.

Les renseignements contenus au registre (annexe 7) doivent être tenus à jour et conservés pendant une période minimale de cinq ans suivant la date ou la période au cours de laquelle la Commission a pris connaissance de l'incident.

### 6.8 Suivi des incidents

Le responsable de l'accès doit s'assurer de la pérennité de l'ensemble des mesures prises pour réduire les risques qu'un incident se produise de nouveau et pour corriger les lacunes identifiées. À cette fin, il doit :

1. Effectuer une description chronologique des événements et des actions prises dans la foulée de l'incident, y compris les dates et les intervenants concernés sur la fiche d'incident (annexe 1);

2. Évaluer si les mesures prises sont adéquates pour réduire les risques qu'un incident se produise de nouveau et corriger les lacunes identifiées. Il doit le consigner dans le registre des incidents (annexe 7);

3. Coordonner son action avec celle du CSIO dans le suivi et la prévention des incidents de confidentialité comportant une composante en sécurité de l'information et le consigner dans un rapport à soumettre au Comité AIPRP.

### 6.9 Prévention des incidents

Le responsable de l'accès évalue les conclusions découlant des suivis de la gestion des incidents de confidentialité pour déterminer les mesures de prévention appropriées. Il s'assure de :

1. Formuler des recommandations de stratégies de prévention à moyen et à long terme;

2. Informer le Comité AIPRP et le comité sur la sécurité de l'information des recommandations afin qu'ils puissent entreprendre les démarches nécessaires et déterminer si ces démarches sont suffisantes afin de prévenir les incidents de même nature.;

3. Réviser la procédure, au besoin.

## 7. Rôles et responsabilités

Présidence

La personne qui assume la présidence de la CAI fait le suivi des recommandations incluses dans les rapports produits par le responsable de l'accès quant aux mesures en place et aux mesures de prévention, dans l'intention de promouvoir une culture de prévention et de gestion des risques.

Responsable de l'accès

Le responsable de l'accès veille à l'application de la Procédure, reçoit les signalements d'incidents de confidentialité et dispose de l'autonomie et de l'autorité nécessaires pour évaluer la situation lorsque survient un incident de confidentialité. Il a également l'autorité nécessaire pour exiger l'assistance et la collaboration des gestionnaires et de toute personne à l'emploi de la CAI dans un contexte de gestion d'un incident de confidentialité.

Il est tenu de prendre les mesures nécessaires pour réduire le risque qu'un préjudice soit causé, d'aviser la Direction de la surveillance et les personnes susceptibles de subir un préjudice lorsqu'il y a un risque de préjudice sérieux ou d'aviser tout organisme ou toute personne pouvant aider à atténuer le risque de préjudice sérieux, tout en le consignant dans le registre de communications.

Le responsable de l'accès s'assure de documenter tout incident de confidentialité à l'aide d'une fiche d'incident et de l'inscrire dans le registre des incidents de confidentialité. Il doit également assurer l'intégrité et la fiabilité des données contenues dans ce registre, prendre les mesures nécessaires pour que soit corrigée toute lacune identifiée, formuler des recommandations dans le but de prévenir la survenance des incidents de confidentialité dans un rapport soumis au Comité AIPRP à chacune de ses rencontres.

Le responsable de l'accès informe le Comité AIPRP de tout incident de confidentialité lors de ses réunions statutaires.

Gestionnaire de l'unité concernée par un incident de confidentialité

Le gestionnaire de l'unité concernée par un incident de confidentialité transmet sans délai toutes les informations nécessaires au responsable de l'accès, dès qu'il a des motifs de croire que s'est produit ou qu'a été découvert un incident de confidentialité dans son unité ou à l'extérieur de son unité. Le gestionnaire doit assister le responsable de l'accès et collaborer avec lui dans la gestion de l'incident de confidentialité, faire le suivi et appliquer les mesures nécessaires afin de contenir l'incident et d'éviter qu'il se reproduise.

Comité AIPRP

Le Comité AIPRP collabore avec le responsable de l'accès lors d'un incident. À l'aide des informations transmises par le responsable de l'accès, il recommande les meilleures stratégies pour diminuer le risque de préjudice lors d'un incident et prévenir les incidents de confidentialité de même nature. Il peut aussi recommander des mesures visant à prévenir toute forme d'incident de confidentialité.

Chef organisationnel de la sécurité de l'information (CSIO)

Le CSIO collabore avec le responsable de l'accès dans la prise en charge de la gestion des incidents de confidentialité comportant une composante en sécurité de l'information.

Personnel et membres de la CAI

Un membre du personnel ou un membre de la CAI avise sans délai son supérieur immédiat lorsqu'il a des motifs de croire que s'est produit un incident de confidentialité. Au besoin, il collabore avec le responsable de l'accès dans la prise en charge de la gestion des incidents de confidentialité. Le personnel et les membres de la CAI prennent toute mesure raisonnable pour prévenir la survenance des incidents de confidentialité au sein de l'organisme.

## 8. Entrée en vigueur

La présente Procédure entre en vigueur le 12 juin 2023.

# Annexe 1 : Fiche d’incident


**Fiche d’incident de confidentialité**

---

| 1. CIRCONSTANCES DE L’INCIDENT (DATE, LIEU, QUI A RAPPORTÉ INCIDENT) |
| --- |
| |
| 2. DESCRIPTION DE L’INCIDENT (CONTEXTE, CAUSE, SOURCE) |
| |

| 3. RENSEIGNEMENTS PERSONNELS ET LEUR NATURE |
| --- |
| |
| 4. PERSONNES DONT LES RENSEIGNEMENTS PERSONNELS SONT VISÉS PAR L'INCIDENT |
| **La personne concernée n'a pas à être avisée si cela est susceptible d'entraver une enquête menée par une personne ou un organisme qui, en vertu de la loi, est chargé de prévenir, de détecter ou de réprimer le crime ou les infractions aux lois.* |
| |

## 5. PERSONNES IMPLIQUÉES ET LEURS RÔLES

**La communication des renseignements sera faite sans le consentement de la personne concernée. Cette communication doit être inscrite dans le registre de communications des renseignements nécessaires (annexe 6).*

***Les personnes impliquées peuvent inclure les personnes ayant découvert l'incident, ayant porté assistance, ayant collaboré ou ayant agi de manière à faciliter le travail du responsable de l'accès conformément à la procédure*

## 6. CAUSE(S) DE L'INCIDENT

| | |
|---|---|
| Préparée par : | |
| Collaboration : | |
| Secteur : | |
| Approuvée par : | |
| Approuvée par : | |
| Date : | |

## COMPTE RENDU DU SECTEUR CONCERNÉ

| |
|---|
| 1. CIRCONSTANCES DE L'INCIDENT (DATE, LIEU, QUI A RAPPORTÉ INCIDENT) |
| |
| 2. DESCRIPTION DE L'INCIDENT (CONTEXTE, CAUSE, SOURCE) |
| |
| 3. RENSEIGNEMENTS PERSONNELS IMPLIQUÉS ET LEUR NATURE |
| |
| 4. PERSONNES DONT LES RENSEIGNEMENTS PERSONNELS SONT CONCERNÉS PAR L'INCIDENT |
| **La personne concernée n'a pas à être avisée si cela est susceptible d'entraver une enquête faite par une personne ou par un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois.* |
| |
| 5. PERSONNES IMPLIQUÉES ET LEURS RÔLES |

| |
|---|
| ** La communication sera faite sans le consentement de la personne concernée. La communication doit être inscrite dans le registre de communications des renseignements nécessaires (annexe 6).*<br><br>***Les personnes impliquées peuvent inclure les personnes ayant découvert l'incident, ayant porté assistance, ayant collaboré ou ayant agi de manière à faciliter le travail du responsable de l'accès conformément à la procédure* |
| |
| 6. CAUSE(S) DE L'INCIDENT |
| |

Préparé par :

Date :

## Annexe 2 : Grille d’évaluation du risque de préjudice sérieux


La grille permet d’établir le niveau de préjudice et de documenter la démarche.

1. Date ou période de l’événement : Cliquez ou appuyez ici pour entrer une date.

2. Type d’incident / cause de l’incident :

☐ Accès non autorisé;

☐ Utilisation non autorisée;

☐ Communication non autorisée;

☐ Perte ou autre atteinte à la protection des renseignements personnels.

3. Est-ce que des renseignements personnels sont concernés?

☐ Oui, il s’agit d’un incident de confidentialité (veuillez compléter les questions subséquentes pour évaluer les risques de préjudice);

☐ Non, il s’agit d’un incident de sécurité (veuillez inscrire l’incident au registre des incidents de sécurité, en informer le responsable de la sécurité et continuer l’analyse pour évaluer les conséquences appréhendées et les mesures à prendre).

4. Quelle est la nature des renseignements personnels concernés?

☐ Renseignements d’identification (nom, coordonnées, adresse postale, courriel, numéro de téléphone, numéro d’assurance sociale/maladie, permis de conduire, passeport, code permanent, code d’utilisateur, mot de passe, etc.);

☐ Renseignements financiers (numéro de carte de crédit ou de compte bancaire, salaire, conditions d’emploi, etc.);

☐ Renseignements de santé (dossier médical, âge, taille, poids, plan d’intervention, groupe sanguin, etc.);

☐ Renseignements relatifs au travail (dossier disciplinaire, motifs d'absences, dates de vacances, salaire, évaluation du rendement, heures d'entrée et de sortie liées au lieu de travail, etc.);

☐ Renseignements génétiques ou biométriques (empreintes digitales, signature vocale, ADN, etc.);

☐ Autre (précisez) (combinaison de facteurs pouvant rendre les renseignements sensibles, dont les antécédents judiciaires, le dossier d'employé, etc.) : .

5. Qui détient maintenant les renseignements personnels faisant l'objet de l'incident de confidentialité?

☐ Organisme public;

☐ Citoyen;

☐ Entreprise privée;

☐ Inconnu.

6. Quelles sont les probabilités que ces renseignements personnels soient utilisés à des fins préjudiciables?

☐ Nulles;

☐ Faibles;

☐ Moyennes;

☐ Élevées.

7. Quelles sont les conséquences appréhendées de l'utilisation malintentionnée de ces renseignements personnels?

☐ Vol ou usurpation d'identité;

☐ Fraude ou perte financière;

☐ Répercussion négative sur la santé physique ou psychologique;

☐ Perte d'emploi ou perte d'occasion d'emploi;

☐ Dommages moraux (humiliation, atteinte à la réputation ou à la vie privée, discrimination, diffamation);

☐ Autre (précisez) : ;

☐ Aucune.

8. En fonction de cette évaluation, un risque de préjudice sérieux peut-il être appréhendé?

☐ Oui, continuez l'analyse;

☐ Non, vous n'avez pas à aviser la Direction de la surveillance de la CAI, mais vous devez inscrire l'incident au registre et prendre des mesures pour atténuer le risque de préjudice.

9. Quelles mesures ont été prises pour éviter ou réduire le risque qu'un incident de même nature se reproduise?

☐ Les renseignements personnels ont été récupérés et n'ont pas été consultés;

☐ L'appareil a été effacé à distance et les renseignements n'ont pas été consultés ;

☐ Le problème à l'origine de la violation a été résolu;

☐ Les détenteurs des renseignements personnels ont été contactés;

☐ Autre (précisez) (correction des méthodes de travail, formation, mesures de sécurité administratives, physiques ou techniques, contact avec les autorités policières ou des experts externes, etc.) : ;

☐ Aucune.

10. Quelles sont les mesures mises en place pour empêcher l'accès aux renseignements personnels? (Ex. sécurisation de la clé de cryptage pour déverrouiller des renseignements personnels cryptés, authentification multi-facteurs pour accéder à un compte, protection d'un document à l'aide d'un mot de passe, etc.) :

11. Le responsable de l'accès doit toujours inscrire l'incident au registre des incidents de confidentialité, **et** l'incident doit, s'il présente un risque de préjudice sérieux (plus d'un choix peut s'appliquer) :

☐ Être déclaré avec diligence à la Direction de la surveillance en utilisant le formulaire d'avis de la Commission;

☐ Être communiqué à une personne ou à un organisme susceptible d'atténuer le préjudice*;

☐ Être déclaré aux personnes concernées**.

*Note : *La communication des renseignements sera faite sans le consentement de la personne concernée. La communication doit être inscrite dans le registre de communications des renseignements nécessaires (annexe 6).*

***La personne concernée n'a pas à être avisée si cela est susceptible d'entraver une enquête menée par une personne ou un organisme qui, en vertu de la loi, est chargé de prévenir, de détecter ou de réprimer le crime ou les infractions aux lois. Dans le cas où un avis est nécessaire et que la personne n'est pas joignable ou qu'un tel avis ne lui cause un préjudice additionnel, la Commission peut aviser les personnes concernées au moyen d'un avis public.*

Signature de la personne ayant fait l'évaluation :

Signature du responsable PRP :

Date de l'évaluation :

**Annexe 3 : Avis à la direction de la surveillance CAI**

## Annexe 4 : Avis aux personnes concernées


Montréal (ou Québec), le (date)

(Madame ou Monsieur) (nom)

(adresse)

**Objet : Incident de confidentialité – dossier(s) (numéro de(s) dossier(s) employé(s))**

(Madame ou Monsieur),

Nous vous informons qu'un incident de confidentialité concernant votre dossier employé est survenu le (date).

En effet, (brève description des circonstances de l'incident, incluant la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période).

Les renseignements personnels visés par l'incident sont les suivants : (énumérer la liste des renseignements personnels visés. Si cette information n'est pas connue, fournir la raison justifiant l'impossibilité de fournir la description).

La Commission prend actuellement (ou entend prendre) les mesures suivantes afin de minimiser les risques qu'un préjudice soit causé (brève description des mesures). De plus, nous vous recommandons de (inscrire les mesures que l'organisation suggère à la personne concernée de prendre afin de diminuer le risque qu'un préjudice lui soit causé ou afin d'atténuer un tel préjudice. Par exemple, joindre fiches d'informations de la CAI).

Pour toute information supplémentaire, veuillez vous adresser au soussigné.

Veuillez agréer, Madame (ou Monsieur), nos salutations distinguées.

_____

Jorge Passalacqua

Responsable de l’accès à l’information

et de la protection des renseignements personnels

2045, rue Stanley, bureau 900

Montréal (Québec)  H3A 2V4

Téléphone : 514 873-4196

Télécopieur : 514 -844-6170

Courriel : responsable.acces@cai.gouv.qc.ca

p. j. Fiches d’information de la Commission d’accès à l’information

## Annexe 4 : Avis aux personnes concernées


Montréal (ou Québec), le (date)

(Madame ou Monsieur) (nom)

(adresse)

**Objet : Incident de confidentialité – dossier(s) (numéro de(s) dossier(s))**

(Madame ou Monsieur),

Nous vous informons qu'un incident de confidentialité concernant le(s) dossier(s) (numéros de(s) dossiers(s)), dans le(s)quel(s) vous êtes (requérant(e), mis(e) en cause, impliqué(e)), est survenu le (date).

En effet, (brève description des circonstances de l'incident, incluant la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période).

Les renseignements personnels visés par l'incident sont les suivants : (énumérer la liste des renseignements personnels visés. Si cette information n'est pas connue, fournir la raison justifiant l'impossibilité de fournir la description).

La Commission prend actuellement (ou entend prendre) les mesures suivantes afin de diminuer les risques qu'un préjudice soit causé (brève description des mesures). Aussi, nous vous recommandons de (inscrire les mesures que l'organisation suggère à la personne concernée de prendre afin de diminuer le risque qu'un préjudice lui soit causé ou afin d'atténuer un tel préjudice. Par exemple, joindre fiches d'informations de la CAI).

Pour toute information supplémentaire, veuillez vous adresser au soussigné.

Veuillez agréer, Madame (ou Monsieur), nos salutations distinguées.

_____

Jorge Passalacqua

Responsable de l’accès à l’information

et de la protection des renseignements personnels

2045, rue Stanley, bureau 900

Montréal (Québec)  H3A 2V4

Téléphone : 514 873-4196

Télécopieur : 514 844-6170

Courriel : responsable.acces@cai.gouv.qc.ca

p. j. Fiches d’information de la Commission d’accès à l’information

# Annexe 5 : Avis public


**AVIS PUBLIC**

(Lieu), le (date) - Conformément à l'article 49 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1) (la Loi), la Commission avise publiquement le tiers (préciser le nom du tiers) qu'un incident de confidentialité concernant le(s) dossier(s) (numéros de(s) dossiers(s)), dans le(s)quel(s) ils sont (requérants(es), mis(es) en cause, impliqués(es)), est survenu le (date).

Nous vous invitons à communiquer avec (nom du responsable), responsable de l'accès aux documents, au numéro suivant : (préciser), afin que nous puissions vous fournir des précisions additionnelles sur l'incident.

## Annexe 6 : Registre des communications des renseignements en lien avec des incidents de confidentialité en vertu de l'article 63.8 LAI


**Registre de communications des renseignements en lien avec des incidents de confidentialité**

(en vertu de l'article 63.8 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*)

| Numéro de(s) dossier(s) | Date de la communication | Circonstances de l'incident | Renseignements personnels communiqués | Personne ou organisme receveur et ses coordonnées | Objectifs de la démarche |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Commission d'accès à l'information du Québec

# Annexe 7 : Registre des incidents de confidentialité

| Registre des incidents de confidentialité 2023-2024 | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Numéro de(s) dossier(s) | Date ou période de l'incident (AAAA-MM-JJ) | Date de prise de connaissance de l'incident (AAAA-MM-JJ) | Date de l'avis de l'incident au responsable de la protection des renseignements personnels (AAAA-MM-JJ) | Nature des RP visés par l'incident | Description des circonstances de l'incident | Nombre de personnes concernées par l'incident | Description des éléments qui mènent à conclure qu'il existe ou non un risque qu'un préjudice sérieux soit causé aux personnes concernées | Date de transmission de l'avis aux personnes concernées ou date de transmission d'un avis public, le cas échéant (AAAA-MM-JJ) | Date de transmission de l'avis à toute personne ou à tout organisme susceptible d'atténuer le risque | Mesures de mitigation immédiates et description des mesures prises afin de diminuer les risques qu'un préjudice soit causé | Description des mesures déployées, afin d'éviter que l'incident se reproduise | Date de l'avis à la Commission (DS) (AAAA-MM-JJ) | Commentaires |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |

## Annexe 8 : Liste des personnes répondantes en matière de PRP

Commission d'accès à l'information du Québec

| Unité | Personne répondante | Fonction | Coordonnées |
|---|---|---|---|
| Direction des affaires institutionnelles, des communications et de la promotion (DAICP) | Jorge Passalacqua | Directeur et responsable de l'accès | 514 873-4196, poste 52601<br>514 502-6631<br>jorge.passalacqua@cai.gouv.qc.ca |
| Direction des affaires institutionnelles, des communications et de la promotion (DAICP) | Catherine-Isabelle Valois | Substitute au responsable de l'accès | 514 873-4196, poste 52602<br>catherine-isabelle.valois@cai.gouv.qc.ca |
| Direction de l'administration | Rémi Bédard | Directeur et Chef de la sécurité de l'information organisationnelle | 418 528-7741, poste 51401<br>remi.bedard@cai.gouv.qc.ca |
| Direction de l'administration | Éric Boivin | Analyste en ressources informationnelles | 418 528-7741, poste 51406<br>eric.boivin@cai.gouv.qc.ca |
| Secrétariat général et direction des affaires juridiques | Jean-Sébastien Desmeules | Directeur | 418 528-7741, poste 51206<br>jean-sebastien.desmeules@cai.gouv.qc.ca |
| Direction de la surveillance | Ralitsa Dimova | Directrice | 418 528-7741, poste 51310<br>ralitsa.dimova@cai.gouv.qc.ca |

Commission
d'accès à l'information
du Québec

# Procédure de traitement des plaintes relatives à la protection des renseignements personnels

Le 20 septembre 2023

# Table des matières

# 1 Contexte

La Commission d'accès à l'information (la Commission) est à la fois un tribunal administratif et un organisme de surveillance qui veille, entre autres, à l'application de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (c. A-2.1; la Loi sur l'accès) et est également assujettie à cette loi. En vertu de la Loi sur l'accès, les personnes qui considèrent que la gestion de leurs renseignements personnels par la Commission n'est pas conforme à la législation applicable peuvent porter plainte au responsable de l'accès aux documents et de la protection des renseignements personnels (le responsable de l'accès).

# 2 Objectifs

La présente procédure précise comment porter plainte au sujet des pratiques de la Commission relatives à la protection des renseignements personnels qu'elle détient. Elle précise aussi comment ces plaintes sont traitées et définit les rôles et les responsabilités des membres et du personnel de la Commission à ce chapitre. Le cas échéant, elle prévoit des mesures pour améliorer sa gestion des renseignements personnels à la lumière des situations portées à son attention.

# 3 Champ d'application

La présente procédure s'applique aux renseignements personnels détenus par la Commission et à toute personne qui traite ces renseignements. Les membres de la Commission et son personnel, y compris les étudiants, les stagiaires et les contractuels, sont tenus de se conformer à la présente procédure.

# 4 Définitions

Aux fins de la présente procédure, on entend par :

Personne plaignante : personne physique qui dépose une plainte conformément à la Procédure de traitement des plaintes relatives à la protection des renseignements personnels.

Plainte : insatisfaction d'une personne physique, signifiée par écrit, concernant une pratique de la Commission concernant la protection de ses renseignements personnels.

Renseignement personnel : renseignement concernant une personne physique et permettant de l'identifier directement ou indirectement.

Renseignement personnel sensible : renseignement personnel qui, par sa nature, notamment médicale, biométrique ou autrement intime, ou en raison

du contexte de son utilisation ou de sa communication, suscite un haut degré d'attente raisonnable en matière de vie privée.

# 5 Procédure de traitement des plaintes

## 5.1 Traitement confidentiel de la plainte

Dans le cadre du traitement des plaintes, la Commission s'engage à respecter la confidentialité et à assurer la protection des renseignements personnels qu'elle détient tout au long de leur cycle de vie, de la collecte jusqu'à la destruction.

Toute plainte est traitée de façon confidentielle. Seule l'information nécessaire au traitement de la plainte sera partagée avec les membres du personnel de la Commission qui doivent en prendre connaissance dans l'exercice de leurs fonctions.

## 5.2 Réception de la plainte

Toute plainte concernant la gestion des renseignements personnels par la Commission doit être faite par écrit, adressée au responsable de l'accès et transmise par courriel à responsable.acces@cai.gouv.qc.ca ou par la poste à l'une des adresses suivantes :

**Québec**
Commission d'accès à l'information
Bureau 2.36
525, boulevard René-Lévesque Est
Québec (Québec) G1R 5S9

**Montréal**
Commission d'accès à l'information
Bureau 900
2045, rue Stanley
Montréal (Québec) H3A 2V4

Tout membre du personnel de la Commission saisi d'une plainte doit la transmettre, dès sa réception, au responsable de l'accès. Ce dernier doit accuser réception de la plainte dans les cinq (5) jours ouvrables suivant sa réception.

## 5.3 Recevabilité d'une plainte

Une plainte est recevable si :

- elle est formulée par une personne physique;
- elle concerne une insatisfaction relative à une pratique, une action ou l'inaction de la Commission quant à la gestion ou la protection des renseignements personnels qu'elle détient à son sujet;
- elle contient les éléments suivants :
  - nom, prénom et coordonnées de la personne plaignante;
  - une description suffisamment précise de la situation problématique;
  - la ou les mesures correctrices souhaitées.

Une plainte n'est pas recevable si elle :

- est anonyme;
- est abusive, frivole ou manifestement faite de mauvaise foi;
- contient des propos à caractère haineux ou diffamatoire;
- ne contient pas les informations et précisions nécessaires à son traitement;
- concerne une insatisfaction relative à un sujet autre que la protection des renseignements personnels, par exemple :
    - les décisions des membres et du personnel de la Commission qui interprètent la portée des dispositions légales de la Loi sur l'accès, de la *Loi sur la protection des renseignements personnels dans le secteur privé* (c. P-39.1; la Loi sur le privé) et des autres lois qui doivent être interprétées par la Commission;
    - toute décision relative à la gestion de l'instance sous la responsabilité d'un juge administratif de la section juridictionnelle de la Commission;
    - toute plainte relative au processus d'adjudication ou d'attribution d'un contrat public par la Commission.

Aussi, ne sera pas traitée selon la présente procédure toute démarche informelle visant à faire corriger un problème particulier, dans la mesure où le problème est traité dans le cadre des activités régulières de la Commission et sans qu'une plainte écrite n'ait été déposée par une personne physique.

Une plainte formulée en vertu de la présente procédure ne permet pas l'obtention d'un dédommagement pour la personne plaignante.

Le responsable de l'accès informe la personne plaignante, par écrit, lorsque sa plainte est irrecevable. La lettre précise en quoi la plainte n'est pas recevable.

Lorsque la plainte est recevable, le responsable de l'accès procède au traitement de la plainte. Après l'avoir analysé et recueilli l'ensemble des faits pertinents, il détermine si elle fondée ou non et, le cas échéant, si des mesures correctrices ou des interventions doivent être réalisées.

### 5.4 Détermination du caractère fondé d'une plainte

Une plainte est fondée lorsque le responsable de l'accès conclut à une erreur ou un manquement en lien avec des lois, règlements ou politiques encadrant la gestion et la protection des renseignements personnels par la Commission.

Le responsable peut alors recommander au comité sur l'accès et la protection des renseignements personnels de la Commission (le Comité) des mesures visant à corriger la situation ou à éviter qu'une telle situation ne se reproduise.

Il procède annuellement à l'analyse des plaintes relatives à la protection des renseignements personnels reçues dans l'année et soumet un rapport au Comité qui peut contenir des recommandations en vue d'améliorer les pratiques de gestion des renseignements personnels de la Commission.

### 5.5 Délai de traitement d'une plainte

Le traitement doit être effectué dans les 45 jours suivant la réception de tous les renseignements nécessaires à son traitement. Lorsque la plainte ne peut être traitée dans le délai prévu, le responsable de l'accès informe le plaignant des motifs du retard et du délai dans lequel ses conclusions lui seront transmises.

Lorsque le traitement de la plainte est complété, le responsable transmet par écrit ses conclusions à la personne plaignante. Il indique :

- si la plainte est fondée ou non;
- si elle est fondée, il indique les mesures correctrices recommandées ou les interventions réalisées, le cas échéant.

### 5.6 Registre des plaintes

Le responsable de l'accès doit consigner dans le registre des plaintes toute plainte relative à la protection des renseignements personnels (annexe 1). Le registre doit contenir les renseignements suivants :

- numéro de dossier(s);
- nom, prénom et coordonnées de la personne plaignante;
- date de réception de la plainte par le responsable;
- conclusion quant à sa recevabilité ou non;
- description de la plainte et renseignements personnels visés;
- démarches entreprises;
- date de réponse à la personne plaignante;
- conclusion au sujet du caractère fondé ou non de la plainte;
- recommandations ou autres mesures correctrices réalisées, le cas échéant;
- commentaires.

# 6 Rôles et responsabilités

## La présidence :

- approuve la présente procédure et veille à son application;
- s'assure que le Comité apporte le suivi nécessaire aux rapports produits par le responsable de l'accès relativement à la protection des renseignements personnels;
- traite toute insatisfaction ou plainte mettant en cause le responsable en lien avec la protection des renseignements personnels et informe la personne plaignante du résultat du traitement de son insatisfaction.

## Le responsable de l'accès et de la protection des renseignements personnels :

- reçoit les plaintes et en détermine la recevabilité en conformité avec la présente procédure;
- communique avec la personne plaignante dans les meilleurs délais et l'informe de la façon dont sa plainte sera traitée ainsi que des démarches qui seront entreprises;
- informe la personne plaignante de ses conclusions et de ses démarches, le cas échéant;
- formule des recommandations et des pistes d'amélioration et signale tout manquement ou toute autre situation qui présente des risques en matière de protection des renseignements personnels au comité sur l'accès et la protection des renseignements personnels;
- consigne dans le registre des plaintes toute plainte relative à la protection des renseignements personnels;
- procède annuellement à l'analyse des plaintes relatives à la protection des renseignements personnels reçues dans l'année et soumet un rapport au comité sur l'accès et la protection des renseignements personnels. Il peut formuler des recommandations en vue d'améliorer les pratiques de gestion des renseignements personnels détenus par la Commission.

## Le comité sur l'accès et la protection des renseignements personnels :

- approuve la présente procédure;
- analyse les rapports portant sur les plaintes relatives à la protection des renseignements personnels soumis annuellement par le responsable de l'accès;

- détermine les actions à poser, le cas échéant, afin d'améliorer les pratiques de la Commission en matière de gestion des renseignements personnels et formule des recommandations au comité de direction.

### Les gestionnaires :

- assurent le respect de la présente procédure au sein de leur unité administrative et voient à ce que les plaintes reçues au sein de leur unité administrative soient transmises au responsable de l'accès;
- collaborent avec le responsable de l'accès dans le cadre du traitement des plaintes, au besoin.

## 7 Mise à jour, approbation et entrée en vigueur

La présente procédure est mise à jour au moins tous les cinq (5) ans. Elle peut être révisée avant cette échéance notamment lorsque des changements à la Loi sur l'accès doivent être pris en compte ou que des précisions supplémentaires sont jugées nécessaires. Toute modification à son contenu doit recevoir les approbations nécessaires. La présente procédure entre en vigueur le 20 septembre 2023.

## 8 Encadrement légal, règlementaire et administratif

La présente procédure tient compte des obligations qui découlent des textes suivants :

- la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*;
- la Politique de gestion des renseignements personnels de la Commission;
- la Procédure de gestion des incidents de confidentialité de la Commission.

## Annexe 1 : Registre des plaintes relatives à la protection des renseignements personnels

**Registre des plaintes relatives à la protection des renseignements personnels**

| Numéro de dossier(s) | Nom, prénom et coordonnées de la personne plaignante | Date de réception de la plainte par le responsable | Conclusion quant à sa recevabilité ou non | Description de la plainte et renseignements personnels visés | Démarches entreprises | Date de réponse à la personne plaignante | Conclusion du caractère fondé ou non de la plainte | Notes et recommandations ou autres mesures correctrices réalisées |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

# DIRECTIVE SUR LES SONDAGES RÉALISÉS PAR LA COMMISSION D'ACCÈS À L'INFORMATION OU L'UN DE SES PRESTATAIRES DE SERVICES

MAI 2008

**OBJET**

1. Cette directive a pour but d'établir les exigences minimales applicables à la Commission d'accès à l'information quant à la protection des renseignements personnels lors de sondages impliquant la cueillette ou la communication de renseignements personnels, qu'ils soient réalisés par une unité administrative de la Commission, un membre du personnel de cette unité ou un prestataire de services de la Commission.

**CADRE RÉGLEMENTAIRE**

2. Cette directive est établie conformément aux dispositions de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (ci-après la « Loi sur l'accès ») et de la *Loi sur les archives.*

**UNITÉ OU PERSONNE VISÉE**

3. Cette directive s'applique à tout le personnel de la Commission et, dans la mesure prévue au contrat, à toute personne dûment mandatée à réaliser un sondage au nom de la Commission.

**DÉFINITIONS**

4. Dans la présente directive, on entend par :

   *Renseignements personnels* :

   tout renseignement qui concerne une personne physique et qui permet de l'identifier. Notamment, par exemple : numéro d'assurance sociale, numéro d'assurance maladie, nom, date de naissance, numéro d'identification personnelle, numéro de réclamation, statut civil, adresse personnelle, numéro de téléphone.

   *Renseignements sensibles* :

   tout renseignement personnel concernant notamment la santé, la religion, l'orientation sexuelle ou les opinions politiques.

**AVIS LORS DE LA CUEILLETTE DE RENSEIGNEMENTS PERSONNELS**

5. Dès le moment où un membre du personnel de la Commission recueille des renseignements personnels nécessaires à l'exercice des attributions de la Commission ou à la mise en œuvre d'un programme dont il a la gestion, celui-ci doit informer les personnes concernées que ces renseignements pourront être utilisés à des fins de recherche, d'évaluation ou d'enquête et qu'un recours aux techniques de sondage est possible.

**MODALITÉS D'APPLICATION**

6. Avant la réalisation d'un sondage par la Commission impliquant l'utilisation ou la cueillette de renseignements personnels, sans recourir à un prestataire de services, le gestionnaire de l'unité administrative doit :

   a) procéder, avec le concours du responsable de la protection des renseignements personnels, à une évaluation éthique du projet de sondage si des renseignements personnels

sensibles peuvent être recueillis dans le cadre du sondage;

b) vérifier, avec le concours du responsable de la protection des renseignements personnels, les situations où il est requis d'obtenir le consentement des personnes concernées par les renseignements;

c) s'assurer qu'il est impossible d'obtenir le consentement des personnes concernées par les renseignements personnels;

d) s'assurer que seuls les renseignements nécessaires à la réalisation du sondage seront utilisés et recueillis.

7. Lorsque le sondage est réalisé par un prestataire de services de la Commission, le gestionnaire de l'unité administrative qui désire faire réaliser ce sondage doit, avant de communiquer des renseignements personnels à ce prestataire :

a) vérifier auprès du responsable de la protection des renseignements personnels si la Loi sur l'accès ou une disposition quelconque d'une loi dont la responsabilité incombe à la Commission ne comporte pas de dispositions qui l'empêchent de communiquer des renseignements personnels à un prestataire de services;

b) vérifier, avec le concours du responsable de la protection des renseignements personnels, si la communication de renseignements personnels au prestataire de services est nécessaire à la réalisation du sondage;

c) effectuer une évaluation éthique du projet de sondage, en collaboration avec le responsable de la protection des renseignements personnels, si des renseignements sensibles doivent être communiqués à un prestataire de services ou recueillis par ce dernier, lors d'un sondage;

d) s'assurer qu'il est impossible d'obtenir le consentement des personnes concernées par la communication des renseignements personnels, lorsqu'une telle communication est requise aux fins de permettre au prestataire de services d'exécuter son contrat;

e) prendre les mesures appropriées pour que seuls les renseignements nécessaires à la réalisation du sondage soient communiqués;

f) identifier, avec le concours du responsable de la protection des renseignements personnels, les renseignements personnels qui devront faire l'objet d'une inscription au registre tenu conformément à l'article 67.3 de la Loi sur l'accès.

**RÉDACTION DU CONTRAT**

8. Le contrat de réalisation d'un sondage doit respecter les conditions et modalités imposées par l'article 67.2 de la Loi sur l'accès. Ce contrat doit :

   a) être fait par écrit et comporter la clause visée par l'annexe 1 de la présente directive;

   b) préciser que les renseignements personnels communiqués sont confidentiels et quels sont les articles de la Loi sur l'accès qui s'appliquent à ces renseignements (annexe 2);

   c) préciser les mesures qui seront prises pour s'assurer que les renseignements personnels ne seront utilisés que pour les fins de la réalisation du contrat;

   d) préciser qu'au terme du contrat les renseignements personnels communiqués par la Commission et ceux recueillis dans le cadre du sondage lui seront retournés ou seront détruits par le prestataire de services;

   e) prévoir le respect de la confidentialité des renseignements colligés par le prestataire de services et le respect des obligations d'information énoncées à l'article 65 de la Loi sur l'accès si le prestataire collige, au nom de la Commission, des renseignements personnels;

   f) exiger du prestataire et de son personnel qu'ils s'engagent à respecter les dispositions de la présente directive;

   g) stipuler que le contractant doit obtenir l'autorisation écrite de la Commission pour confier, en partie, à un sous-traitant la réalisation du sondage comportant la communication de renseignements personnels.

**SOUS-TRAITANCE**

9. Le contractant qui retient les services d'un sous-traitant pour la réalisation du sondage doit conclure un contrat écrit avec ce dernier.

   La Commission doit être partie à ce contrat et le sous-traitant est assimilé au contractant aux fins d'application de la présente directive.

**ENGAGEMENTS DU PRESTATAIRE**

10. Tout contrat conclu avec un prestataire de services doit prévoir certaines dispositions en vertu desquelles ce prestataire ou, le cas échéant, le personnel de ce prestataire s'engage à :

    a) garantir la confidentialité de tout renseignement personnel qui lui est communiqué par la Commission;

    b) prendre, à toute étape de la réalisation du sondage, les mesures de sécurité nécessaires pour assurer la

confidentialité des renseignements apparaissant sur tout document, peu importe son support, qui lui est communiqué ou dont il prend connaissance dans le cadre de l'exécution de son contrat;

c) ne pas faire usage ou permettre qu'il soit fait usage d'un document ou d'un renseignement personnel, à une fin autre que celle prévue par le contrat, à ne pas permettre à quiconque n'est affecté à l'exécution du contrat, de prendre connaissance d'un renseignement personnel dont la communication lui a été révélée, et à ne pas communiquer de renseignement personnel à un tiers;

d) faire signer un engagement, prenant la forme d'une déclaration de discrétion, dont la teneur sera substantiellement conforme à celle apparaissant à l'annexe 3 de la présente directive, à toute personne qui sera affectée à la manipulation ou au traitement des renseignements communiqués par un répondant ou par un membre du personnel de la Commission;

e) faire signer un engagement prenant la forme d'une déclaration de discrétion, dont la teneur sera substantiellement conforme à celle apparaissant à l'annexe 3 de la présente directive, à toute personne chargée de la supervision des personnes mentionnées au paragraphe d);

f) permettre à la Commission de faire, sans préavis, et à tout moment pendant la durée du contrat, une vérification du traitement des renseignements qu'il communique à son prestataire ou que celui-ci a recueillis durant l'exécution de son contrat;

g) aviser sans délai la Commission de toute violation ou tentative de violation par toute personne de l'une ou l'autre des obligations relatives à la confidentialité prévues à la présente directive, à la déclaration de discrétion ou au contrat.

**RÉALISATION DU SONDAGE**

11. Le gestionnaire de l'unité administrative responsable du sondage doit s'assurer, lors de la réalisation d'un sondage, que le prestataire ou tout membre de son personnel respecte le principe du « libre choix » de toute personne sollicitée à répondre aux questions d'un sondage.

Le recours à toute manœuvre qui a pour but de contrer le refus de répondre d'une personne sollicitée doit être proscrit.

Il doit aussi s'assurer que le sondage ne permet de recueillir que les seuls renseignements nécessaires à l'exercice des attributions de la Commission ou à la mise en œuvre d'un programme dont il a la gestion.

12. Lorsqu'il y a collecte de renseignements personnels, les membres du personnel de la Commission, le gestionnaire de l'unité administrative concernée ou le prestataire doivent :

a) s'identifier;

b) mentionner que la collecte des renseignements est effectuée au nom de la Commission;

c) informer la personne sollicitée des fins auxquelles le renseignement est destiné (recherche, évaluation, enquête);

d) informer la personne sollicitée du caractère facultatif de sa participation au sondage;

e) informer la personne sollicitée des droits d'accès et de rectification prévus à la Loi sur l'accès et de l'endroit où elle pourra les exercer.

**TRAITEMENT DES RENSEIGNEMENTS PERSONNELS COMMUNIQUÉS OU RECUEILLIS ET PUBLICATION DES RÉSULTATS**

13. Au terme de la réalisation d'un sondage par le prestataire, le gestionnaire de l'unité administrative concernée de la Commission doit :

a) s'assurer que les renseignements personnels communiqués au prestataire pour la réalisation du sondage lui soient retournés ou aient été détruits;

b) s'assurer que les renseignements personnels recueillis par le prestataire à la faveur du sondage lui ont été remis et que le prestataire n'en garde aucune trace;

c) s'assurer que le prestataire, conformément au guide ci-joint adopté par la Commission d'accès à l'information et intitulé *Guide pour la destruction des documents renfermant des renseignements personnels - janvier 1995*, procède à une destruction totale des renseignements qu'il détient et qu'il lui fasse rapport de cette destruction en complétant l'annexe 4 et ce, aux fins du paragraphe a) du présent article;

d) s'assurer que le prestataire s'engage à ne pas se départir, entre les mains d'un tiers, d'un document détenu sur support papier contenant des renseignements personnels communiqués ou recueillis, sauf si la remise de ce document est effectuée aux fins d'en assurer la destruction complète et sécuritaire conformément au guide adopté par la Commission identifié au paragraphe précédent;

e) s'assurer que le prestataire s'engage à ne pas se départir, entre les mains d'un tiers, d'un document détenu sur support électronique contenant des renseignements personnels communiqués ou recueillis, sauf si la remise de

ce document est effectuée aux fins d'en assurer la destruction complète et sécuritaire et que la méthode ou le moyen de destruction utilisé ne permette d'aucune façon la récupération des renseignements, même à l'aide d'un utilitaire approprié et obtenir du prestataire l'attestation de destruction de l'annexe 4.

14. Si une unité administrative de la Commission recueille des renseignements personnels à la faveur d'un sondage réalisé par son personnel ou son prestataire, le gestionnaire de cette unité doit :

    a) prendre les mesures de sécurité qui s'imposent pour assurer le caractère confidentiel de ces renseignements;

    b) prendre les mesures pour s'assurer que les renseignements sont accessibles aux seules personnes à qui ces renseignements sont nécessaires dans l'exercice de leurs fonctions;

    c) s'assurer que les renseignements ne seront utilisés qu'aux seules fins pour lesquelles ils ont été recueillis soit des fins de recherche, d'évaluation ou d'enquête;

    d) s'assurer que les renseignements ne seront pas versés dans d'autres fichiers de renseignements personnels;

    e) s'assurer que la publication des résultats de toute recherche, évaluation ou enquête ne contient pas de renseignements personnels;

    f) s'assurer que le calendrier de conservation des documents de l'organisme prévoit une durée de conservation et un mode de disposition (destruction, conservation ou tri par échantillonnage ou sélection) pour ces renseignements personnels.

15. Si les renseignements recueillis à la faveur d'un sondage peuvent avoir un impact direct sur le droit d'une personne à un service ou à une allocation, le gestionnaire de l'unité administrative concernée doit :

    a) prendre des mesures additionnelles et précises pour déterminer les droits d'accès à ces renseignements;

    b) limiter les droits d'accès aux seules personnes chargées des projets de recherche, d'évaluation ou d'enquête, de même qu'à la personne concernée par ces renseignements.

**RÔLE DU RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS**

16. Le responsable de la protection des renseignements personnels de la Commission doit être étroitement associé à chacune des étapes de la réalisation d'un sondage qui implique la cueillette et la communication de renseignements personnels, qu'il soit réalisé par la Commission ou l'un de ses prestataires.

**RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS**

17. Il incombe au responsable de la protection des renseignements personnels d'aider le personnel à mieux circonscrire l'interprétation et l'administration de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* relativement à toute situation impliquant la cueillette, la communication, la conservation et la destruction de renseignements personnels.

**OBLIGATION DU GESTIONNAIRE**

18. Le gestionnaire d'une unité administrative de la Commission qui désire faire réaliser un sondage par les membres de son unité administrative doit s'assurer que ceux-ci ont une connaissance adéquate du contenu de la présente directive.

    Il doit également communiquer cette directive à tout prestataire à qui il désire confier le contrat de réaliser un sondage.

**ENTRÉE EN VIGUEUR**

19. La présente directive entre en vigueur à la date de signature par le président de la Commission.

**DATE :**_____

_____

Me Jacques St-Laurent
Président de la Commission d'accès à l'information

**Clause type**

L'entreprise reconnaît le caractère confidentiel des renseignements personnels qui lui sont communiqués ou qui seront recueillis pour la réalisation du sondage. Elle s'engage, en conséquence, à prendre connaissance et à respecter la Loi sur l'accès, en particulier les articles 53, 54, 59, 64, 65, 67.2 et 89 de cette loi.

Les renseignements personnels suivants sont communiqués à l'entreprise :

A :
B :

L'entreprise reconnaît avoir lu et compris les dispositions de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q., c. A-2.1) susmentionnées.

L'entreprise s'engage, ainsi que son personnel, à respecter les exigences de la directive sur les sondages, celle-ci faisant partie intégrante du présent contrat (annexe II).

Considérant que les renseignements personnels sont confidentiels et afin d'assurer cette confidentialité lorsque des renseignements personnels sont communiqués au contractant pour la réalisation du contrat et, le cas échéant, lorsque des renseignements personnels sont recueillis à l'occasion de sa réalisation, l'entreprise s'engage à :

1. garantir la confidentialité de tout renseignement personnel qui lui est communiqué par la Commission;
2. prendre, à toute étape de la réalisation du sondage, les mesures de sécurité nécessaires pour assurer la confidentialité des renseignements apparaissant sur tout document, peu importe son support, qui lui est communiqué ou dont il prend connaissance dans le cadre de l'exécution de son contrat;
3. ne pas faire usage ou permettre qu'il soit fait usage d'un document ou d'un renseignement personnel à une fin autre que celle prévue par le contrat, à ne pas permettre à quiconque n'est affecté à l'exécution du contrat de prendre connaissance d'un renseignement personnel dont la communication lui a été révélée et à ne pas communiquer de renseignement personnel à un tiers;
4. informer son personnel des obligations stipulées à la présente disposition et diffuser à cet égard toute l'information pertinente;
5. rendre accessibles les renseignements personnels, au sein des membres de son personnel, uniquement à ceux qui ont qualité pour les recevoir, lorsqu'ils sont nécessaires à l'exercice de leurs fonctions;
6. faire signer aux membres de son personnel des engagements au respect de la confidentialité des renseignements personnels, selon le formulaire joint en annexe au contrat, et les transmettre à la Commission;

7. ne communiquer les renseignements personnels, sans le consentement de la personne concernée, à qui que ce soit, sauf dans le cadre d'un contrat de sous-traitance et selon les modalités prévues à l'article 9 de la directive sur les sondages;
8. soumettre à l'approbation de la Commission le formulaire de consentement à la communication de renseignements personnels de la personne concernée;
9. utiliser les renseignements personnels uniquement pour la réalisation du contrat;
10. recueillir un renseignement personnel au nom de la Commission dans les seuls cas où cela est nécessaire à la réalisation du contrat et informer préalablement toute personne visée par cette cueillette de l'usage auquel ce renseignement est destiné, ainsi que des autres éléments mentionnés à l'article 65 de la Loi sur l'accès;
11. prendre toutes les mesures de sécurité propres à assurer la confidentialité des renseignements personnels à toutes les étapes de la réalisation du contrat;
12. ne conserver à l'expiration du contrat aucun document contenant un renseignement personnel, quel que soit le support, en les retournant à la Commission ou en procédant, aux frais de l'entreprise, à leur destruction conformément au *Guide pour la destruction des documents renfermant des renseignements personnels – janvier 1995 – CAI* dont l'entreprise déclare avoir reçu copie;
13. informer dans les plus brefs délais la Commission de tout manquement aux obligations prévues à la présente disposition ou de tout événement pouvant risquer de porter atteinte à la sécurité ou à la confidentialité des renseignements personnels;
14. fournir à la demande de la Commission toute l'information pertinente au sujet de la protection des renseignements personnels et l'autoriser à visiter les lieux où l'entreprise détient les renseignements personnels afin de s'assurer du respect de la présente disposition;
15. lorsque la réalisation du présent contrat est confiée à un sous-traitant et qu'elle comporte la communication ou la cueillette de renseignements personnels, obtenir l'autorisation écrite de la Commission qui doit être partie au contrat de sous-traitance;
16. permettre à la Commission de faire, sans préavis, et à tout moment pendant la durée du contrat, une vérification du traitement des renseignements qu'il communique à son prestataire de services ou que celui-ci a recueillis durant l'exécution de son contrat.

Dans l'éventualité où le sous-traitant est en défaut de respecter ses obligations relatives à la protection des renseignements personnels, la Commission se réserve le droit de résilier le contrat intervenu avec l'entreprise.

**Extraits de la Loi sur l'accès**

**53.** Les renseignements personnels sont confidentiels sauf dans les cas suivants:

1° la personne concernée par ces renseignements consent à leur divulgation; si cette personne est mineure, le consentement peut également être donné par le titulaire de l'autorité parentale;

2° ils portent sur un renseignement obtenu par un organisme public dans l'exercice d'une fonction juridictionnelle; ils demeurent cependant confidentiels si l'organisme les a obtenus alors qu'il siégeait à huis-clos ou s'ils sont visés par une ordonnance de non-divulgation, de non-publication ou de non-diffusion.

**54.** Dans un document, sont personnels les renseignements qui concernent une personne physique et permettent de l'identifier.

**59.** Un organisme public ne peut communiquer un renseignement personnel sans le consentement de la personne concernée.

Toutefois, il peut communiquer un tel renseignement sans le consentement de cette personne, dans les cas et aux strictes conditions qui suivent:

1° au procureur de cet organisme si le renseignement est nécessaire aux fins d'une poursuite pour infraction à une loi que cet organisme est chargé d'appliquer, ou au Directeur des poursuites criminelles et pénales si le renseignement est nécessaire aux fins d'une poursuite pour infraction à une loi applicable au Québec;

2° au procureur de cet organisme, ou au Procureur général lorsqu'il agit comme procureur de cet organisme, si le renseignement est nécessaire aux fins d'une procédure judiciaire autre qu'une procédure visée dans le paragraphe 1°;

3° à un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois, si le renseignement est nécessaire aux fins d'une poursuite pour infraction à une loi applicable au Québec;

4° à une personne à qui cette communication doit être faite en raison d'une situation d'urgence mettant en danger la vie, la santé ou la sécurité de la personne concernée;

5° à une personne qui est autorisée par la Commission d'accès à l'information, conformément à l'article 125, à utiliser ce renseignement à des fins d'étude, de recherche ou de statistique;

6° *(paragraphe abrogé);*

7° *(paragraphe abrogé);*

8° à une personne ou à un organisme, conformément aux articles 61, 66, 67, 67.1, 67.2, 68 et 68.1;

9° à une personne impliquée dans un événement ayant fait l'objet d'un rapport par un corps de police ou par une personne ou un organisme agissant en application d'une loi qui exige un rapport de même nature, lorsqu'il s'agit d'un renseignement sur l'identité de toute autre personne qui a été impliquée dans cet événement, sauf s'il s'agit d'un témoin, d'un dénonciateur ou d'une personne dont la santé ou la sécurité serait susceptible d'être mise en péril par la communication d'un tel renseignement.

**64.** Nul ne peut, au nom d'un organisme public, recueillir un renseignement personnel si cela n'est pas nécessaire à l'exercice des attributions de cet organisme ou à la mise en oeuvre d'un programme dont il a la gestion.

Un organisme public peut toutefois recueillir un renseignement personnel si cela est nécessaire à l'exercice des attributions ou à la mise en oeuvre d'un programme de l'organisme public avec lequel il collabore pour la prestation de services ou pour la réalisation d'une mission commune.

La collecte visée au deuxième alinéa s'effectue dans le cadre d'une entente écrite transmise à la Commission. L'entente entre en vigueur 30 jours après sa réception par la Commission.

**65.** Quiconque, au nom d'un organisme public, recueille verbalement un renseignement personnel auprès de la personne concernée doit se nommer et, lors de la première collecte de renseignements et par la suite sur demande, l'informer:

1° du nom et de l'adresse de l'organisme public au nom de qui la collecte est faite;

2° des fins pour lesquelles ce renseignement est recueilli;

3° des catégories de personnes qui auront accès à ce renseignement;

4° du caractère obligatoire ou facultatif de la demande;

5° des conséquences pour la personne concernée ou, selon le cas, pour le tiers, d'un refus de répondre à la demande;

6° des droits d'accès et de rectification prévus par la loi.

L'information qui doit être donnée en vertu des paragraphes 1° à 6° du premier alinéa doit être indiquée sur toute communication écrite qui vise à recueillir un renseignement personnel.

Dans le cas où les renseignements personnels sont recueillis auprès d'un tiers, celui qui les recueille doit se nommer et lui communiquer l'information visée aux paragraphes 1°, 5° et 6° du premier alinéa.

Toutefois, une personne dûment autorisée par un organisme public qui détient des dossiers ayant trait à l'adoption de personnes et qui recueille un renseignement relatif aux antécédents d'une personne visée dans l'un de ces dossiers ou permettant de retrouver un parent ou une personne adoptée n'est pas tenue d'informer la personne concernée ou le tiers de l'usage auquel est destiné le renseignement ni des catégories de personnes qui y auront accès.

Le présent article ne s'applique pas à une enquête de nature judiciaire, ni à une enquête ou à un constat faits par un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois.

**67.2.** Un organisme public peut, sans le consentement de la personne concernée, communiquer un renseignement personnel à toute personne ou à tout organisme si cette communication est nécessaire à l'exercice d'un mandat ou à l'exécution d'un contrat de service ou d'entreprise confié par l'organisme public à cette personne ou à cet organisme.

Dans ce cas, l'organisme public doit:

1° confier le mandat ou le contrat par écrit;

2° indiquer, dans le mandat ou le contrat, les dispositions de la présente loi qui s'appliquent au renseignement communiqué au mandataire ou à l'exécutant du contrat ainsi que les mesures qu'il doit prendre pour en assurer le caractère confidentiel, pour que ce renseignement ne soit utilisé que dans l'exercice de son mandat ou l'exécution de son contrat et pour qu'il ne le conserve pas après son expiration. En outre, l'organisme public doit, avant la communication, obtenir un engagement de confidentialité complété par toute personne à qui le renseignement peut être communiqué, à moins que le responsable de la protection des renseignements personnels estime que cela n'est pas nécessaire. Une personne ou un organisme qui exerce un mandat ou qui exécute un contrat de service visé au premier alinéa doit aviser sans délai le responsable de toute violation ou tentative de violation par toute personne de l'une ou l'autre des obligations relatives à la confidentialité du renseignement communiqué et doit également permettre au responsable d'effectuer toute vérification relative à cette confidentialité.

Le deuxième alinéa ne s'applique pas lorsque le mandataire ou l'exécutant du contrat est un membre d'un ordre professionnel. De même, le paragraphe 2° du deuxième alinéa ne s'applique pas lorsque le mandataire ou l'exécutant du contrat est un autre organisme public.

**89.** Toute personne qui reçoit confirmation de l'existence dans un fichier d'un renseignement personnel la concernant peut, s'il est inexact, incomplet ou équivoque, ou si sa collecte, sa communication ou sa conservation ne sont pas autorisées par la loi, exiger que le fichier soit rectifié.

ANNEXE 3

**FORMULAIRE D'ENGAGEMENT À LA CONFIDENTIALITÉ**

Je, soussigné(e), _____, exerçant mes fonctions au sein de la firme _____, dont la principale place d'affaires est située _____

_____, déclare solennellement ce qui suit :

1° je suis une personne assignée de la firme _____

_____ pour la réalisation du sondage faisant l'objet du contrat intervenu entre celle-ci et la Commission d'accès à l'information;

2° je m'engage solennellement, sans limite de temps, à garder le secret le plus entier, à ne pas communiquer ou permettre que soit communiqué à quiconque quelque renseignement ou document, quel que soit le support, qui me sera communiqué ou dont j'aurai pris connaissance dans l'exercice ou à l'exécution de mes fonctions, à moins d'avoir été dûment autorisé à ce faire par la Commission ou par l'un de ses représentants autorisés;

3° je m'engage également à ne pas faire usage d'un tel renseignement ou document à une fin autre que celle s'inscrivant dans le cadre des rapports contractuels entretenus entre la Commission et _____

_____;

4° j'ai été informé(e) que le défaut par le (la) soussigné (e) de respecter tout ou partie du présent engagement m'expose ou expose la firme de sondage à un recours en justice par la Commission ou ses représentants par suite de tout dommage ou préjudice pouvant en résulter.

**ET J'AI SIGNÉ À _____, CE _____**

_____

(Signature du déclarant)

ANNEXE 4

**Attestation de destruction des renseignements personnels**

Je, soussigné(e), _____exerçant mes fonctions au sein de la firme _____, dont la principale place d'affaires est située au _____
_____
déclare solennellement ce qui suit :

Je suis dûment autorisé(e) par la firme pour certifier que les renseignements personnels communiqués par la Commission d'accès à l'information, ainsi que les renseignements personnels recueillis dans le cadre du contrat portant sur _____

ont été détruits selon les méthodes suivantes :

1 : renseignements sur support papier : par déchiquetage ( )

2 : renseignements sur support informatique : par destruction logique et effacement physique en utilisant un logiciel de réécriture ( )

**ET J'AI SIGNÉ À_____,**
**CE_____,**
**_____.**
**(**signature du déclarant)

Commission
d'accès à l'information
du Québec

# Politique de gestion documentaire

2023-05-31

# Table des matières

## 1. Contexte

La Commission d'accès à l'information (CAI) est un organisme gouvernemental créé le 16 décembre 1982. À l'instar des autres ministères et organismes (MO) du gouvernement, la CAI a des obligations et des responsabilités encadrées du point de vue législatif, réglementaire et administratif, en ce qui a trait à la gestion documentaire.

De façon générale, les MO doivent respecter les lois qui guident l'action des organismes publics en matière d'archives et d'accès à l'information.

La Politique organisationnelle de gestion documentaire (ci-après, la Politique) s'avère la pierre angulaire de la gestion documentaire à la CAI.

Une charte de nommage des documents technologiques, un guide et des procédures en lien avec des aspects spécifiques de la gestion documentaire viennent en appui à la présente Politique.

## 2. Objet

Le principal objectif de la Politique est de doter l'organisation de saines pratiques en gestion documentaire. Ainsi, elle vise à :

- Encadrer l'élaboration, l'application et la mise à jour des outils de gestion documentaire tels que le plan de classification, le calendrier de conservation, la charte de nommage des documents technologiques et le guide de gestion documentaire.
- Définir les rôles et les responsabilités de chacun des intervenants dans les processus de gestion documentaire tels que le classement, le déclassement et la disposition.
- Préserver la mémoire institutionnelle de la CAI.
- Traiter l'information de manière sécuritaire, notamment en respectant les principes de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, ainsi que ceux de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*. Ces lois ont d'autres aspects que la Politique ne prend pas en compte, car ils ne concernent pas directement la gestion documentaire.

## 3. Champ d'application

Cette Politique s'adresse à toutes les personnes employées par la CAI, y compris les étudiants, les stagiaires et les consultants. Elle s'applique à tous les documents, indépendamment du support, ayant une valeur administrative, légale

ou financière et ayant été produits ou reçus par la CAI. Tous documents publiés (possédant un numéro ISBN ou ISSN) visés par le dépôt légal (encadrés par la *Loi sur Bibliothèque et Archives nationales du Québec* (RLRQ, c. B-1.2)) sont exempts de cette Politique.

## 4. Encadrement légal, réglementaire et administratif

L'application de la présente Politique est encadrée par :

- La *Directive gouvernementale sur la sécurité de l'information* (*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 concernant le cadre juridique des technologies de l'information* (RLRQ, c. C-1.1);
- La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (LQ 2021, c. 25);
- 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 protection des renseignements personnels dans le secteur privé* (RLRQ, c. P-39.1);
- La *Loi sur les archives* (RLRQ, c. A-21.1);
- La *Politique administrative concernant la gestion des documents actifs du gouvernement du Québec* (*Loi sur les archives* (RLRQ, c. A-21.1));
- La *Politique administrative concernant la gestion des documents semi-actifs du gouvernement du Québec* (*Loi sur les archives* (RLRQ, c. A-21.1));
- La *Politique de gestion des documents inactifs des organismes publics* (*Loi sur les archives* (RLRQ, c. A-21.1));
- Le *Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques* (RLRQ, c. A-21.1, r. 2).

## 5. Définitions

Arborescence : structure des dossiers (tirée du plan de classification) dans SharePoint.

Authenticité : caractère des données ou des biens dont l'origine, ou, le cas échéant, l'auteur, ainsi que l'intégrité ont été attestés.

Calendrier de conservation : outil qui détermine les périodes d'utilisation et les supports de conservation des documents actifs et semi-actifs d'un organisme et

qui indique quels documents inactifs sont conservés de manière permanente et lesquels sont détruits.

Classement : opération qui consiste à classer les documents en leur attribuant un code de classification approprié afin de faciliter le repérage de l'information.

Cycle de vie : ensemble des étapes (actif, semi-actif, inactif) que franchit un document consigné sur un support, de sa création en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, et ce, jusqu'à sa conservation ou sa destruction, en conformité avec le calendrier de conservation de la CAI.

Déclassement : opération qui consiste à identifier les dossiers qui ont terminé leur stade actif et qui doivent être transférés au stade semi-actif, conformément aux règles de conservation qui y sont rattachées.

Disposition : opération qui consiste à détruire ou à conserver les dossiers qui ont terminé leur stade semi-actif et qui sont devenus inactifs, conformément aux règles de conservation qui y sont rattachées.

Document : information délimitée et structurée de façon tangible ou logique selon le support qui la porte et intelligible sous forme de mots, de sons ou d'images.

Document actif (stade actif) : document qui est couramment utilisé à des fins administratives, légales ou financières.

Document confidentiel : document qui contient des informations sensibles dont l'accès et l'utilisation sont réservés à des personnes ou des entités désignées et autorisées parce qu'elles contiennent des éléments stratégiques ou des renseignements personnels et dont la divulgation non autorisée risquerait de causer des préjudices à l'organisme, à ses partenaires ou à des individus. Pour qu'un document soit considéré comme confidentiel, la notion de préjudice est essentielle.

Document essentiel : document indispensable au fonctionnement d'un organisme public et qui permet d'assurer la continuité ou le rétablissement de ses activités, de ses droits et de ses obligations, en raison d'un événement fortuit et dont la disparition ou la non-disponibilité entraînerait des conséquences graves sur sa capacité à réaliser sa mission.

Document inactif (stade inactif) : document qui n'est plus utilisé à des fins administratives, légales ou financières. Les documents ayant une valeur historique ou de recherche sont versés à Bibliothèque et Archives nationales du Québec (BAnQ). Les autres documents sont détruits.

Document semi-actif (stade semi-actif) : document qui est occasionnellement utilisé à des fins administratives, légales ou financières. Il est à noter que les documents semi-actifs sur support papier doivent être envoyés au Centre gouvernemental de traitement massif (CGTM).

Document technologique : document dont le support fait appel aux technologies de l'information.

Dossier : ensemble de documents susceptibles de fournir une information complète sur une affaire, un sujet, un événement ou une activité.

Équivalence fonctionnelle : capacité de deux ou plusieurs supports technologiques, technologies ou procédés différents à remplir les mêmes fonctions sur le plan juridique.

Gestion documentaire : ensemble des opérations et des techniques se rapportant à la conception, au développement, à l'implantation, à l'application et à l'évolution des systèmes, des outils et des processus administratifs requis pour gérer les documents, et ce, peu importe le support, depuis leur création ou leur réception jusqu'à leur versement à BAnQ ou leur destruction.

Gestion intégrée des documents (GID) : consiste à gérer, **avec un seul logiciel**, les documents, peu importe le support, tout au long de leur cycle de vie.

Intégrité : caractère des données ou des biens qui n'ont subi aucune altération.

Plan de classification : structure hiérarchique et logique des **activités** d'une organisation, allant du général au particulier.

Recevabilité : qualité d'un moyen de preuve ou d'un élément de preuve qui remplit les conditions légales nécessaires à sa prise en considération par le tribunal.

## 6. Principes généraux

La présente Politique couvre tous les processus en gestion documentaire, dont le déroulement est régi par le calendrier de conservation et le plan de classification afin de répondre aux exigences légales. Un guide de gestion documentaire, une charte de nommage des documents technologiques et des procédures de déclassement sont également utilisées.

La CAI confie à la Direction des affaires institutionnelles, des communications et de la promotion (DAICP) le soin de concevoir et de mettre à jour des outils organisationnels de gestion documentaire, en collaboration avec l'ensemble des unités administratives (UA). Elle coordonne l'application de ces outils et offre du soutien aux UA quant à leur utilisation. L'application de la gestion documentaire est uniforme pour l'ensemble des UA de la CAI.

L'accès aux documents est attribué à chaque employé selon ses responsabilités et mandats au sein de son UA.

La sécurité de l'information, les demandes d'accès à l'information et la protection des renseignements personnels sont encadrées par des règles de droit, des normes ou des politiques distinctes auxquelles les employés doivent se référer pour connaître le traitement à accorder aux documents visés.

### 6.1 Plan de classification

Selon la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* :

- L'article 16 prévoit l'obligation, pour tout organisme public, d'établir et de tenir à jour un plan de classification. Ce même article prévoit également qu'un organisme public doit classer ses documents de manière à en permettre le repérage.

Le plan de classification doit évoluer au même rythme que l'organisme public. L'attribution de nouveaux mandats et le transfert de compétences sont des facteurs qui peuvent amener l'organisme public à modifier son plan de classification.

L'utilisation d'un plan de classification offre plusieurs avantages et permet notamment d'atteindre plusieurs objectifs, dont :

- Accélérer le classement des dossiers;
- Favoriser l'accès à l'information en accélérant l'identification et le repérage des documents et des informations qu'ils contiennent;
- Favoriser la prise de décision et la mise en œuvre d'actions de manière plus rapide et plus efficace;
- Diminuer les conséquences de la mobilité du personnel en permettant la continuité des opérations;
- Accroître l'efficience de l'organisme public dans l'accomplissement de ses activités.

### 6.2 Calendrier de conservation

Selon la *Loi sur les archives* :

- L'article 7 prévoit l'obligation, pour tout organisme public, d'établir et de tenir à jour un calendrier de conservation.
- L'article 8 prévoit que tout organisme public doit soumettre à l'approbation de BAnQ un calendrier de conservation et chaque modification.
- L'article 12 prévoit que toute personne qui cesse d'être titulaire d'une fonction au sein d'un organisme public doit laisser sous la garde de cet organisme public tous les documents qu'elle a produits ou reçus en cette qualité, y compris les courriels (traitement des dossiers et échanges entre collègues) reçus ou transmis par un outil de messagerie.
- L'article 13 prévoit que, sous réserve de ce que prévoit le calendrier de conservation de l'organisme public, nul ne peut aliéner ou éliminer un document actif ou semi-actif.

Le calendrier de conservation doit évoluer au même rythme que l'organisme public. L'attribution de nouveaux mandats et le transfert de compétences sont des facteurs qui peuvent amener l'organisme public à modifier son calendrier de conservation.

L'utilisation d'un calendrier de conservation offre plusieurs avantages, dont :

- Des économies en matériel, en espace d'entreposage et en espace de stockage;
- La réduction du temps de recherche, puisqu'il conduit à ne conserver que les documents utiles à la gestion administrative, légale ou financière;
- La diminution de la destruction prématurée de documents et la désignation de ceux dont la conservation permanente doit être assurée.

### 6.3 Numérisation

La numérisation de documents papier est en forte croissance au sein de plusieurs organismes publics. Afin de respecter les exigences légales de la *Loi concernant le cadre juridique des technologies de l'information*, une procédure de numérisation doit être établie.

Pour qu'un document numérisé soit recevable en preuve dans un tribunal, il doit répondre aux exigences des articles 1 et 9 de la *Loi concernant le cadre juridique des technologies de l'information* (ci-dessous) :

Selon la *Loi concernant le cadre juridique des technologies de l'information* :

- L'article 1 prévoit qu'il faut assurer l'équivalence fonctionnelle des documents et leur valeur juridique, quels que soient les supports des documents, ainsi que l'interchangeabilité des supports et des technologies qui les portent.
- L'article 9 prévoit que des documents sur des supports différents ont la même valeur juridique s'ils comportent la même information, si l'intégrité de chacun d'eux est assurée et s'ils respectent les règles de droit qui les régissent.

Les organismes publics assujettis à la *Loi sur les archives* qui procèdent à la numérisation de leurs documents actifs et semi-actifs sont tenus de modifier les règles de conservation touchées par cette opération, en inscrivant au calendrier de conservation un changement de support lié à une numérisation.

### 6.4 Documents essentiels

Un document essentiel est un document indispensable au fonctionnement d'un organisme public et qui permet d'assurer la continuité ou le rétablissement de ses activités, de ses droits et de ses obligations, en raison d'un événement fortuit et

dont la disparition ou la non-disponibilité entraînerait des conséquences graves sur sa capacité à réaliser sa mission.

# 7. Processus en gestion documentaire

## 7.1 Classement

Le classement est l'opération qui consiste à classer les documents selon les activités de la CAI, en leur attribuant le code de classification approprié. Les différents codes de classification se trouvent dans le plan de classification de la CAI.

En ce qui concerne les documents papier, le code de classification doit être inscrit sur la chemise de classement.

Quant aux documents technologiques, ils sont classés dans l'arborescence et un code de classification leur est attribué.

## 7.2 Déclassement

Le déclassement est l'opération qui consiste à identifier les documents qui ont terminé leur stade actif et qui doivent être transférés au stade semi-actif. C'est le calendrier de conservation de la CAI qui détermine la durée de vie des dossiers.

En ce qui concerne les documents papier, une procédure de déclassement devra être produite en considérant les besoins des employés de la CAI, les obligations légales en matière de protection des renseignements personnels et les outils technologiques disponibles (logiciel de gestion documentaire, lecteur réseau, etc.). Il y sera notamment spécifié que ces dossiers doivent être envoyés au Centre gouvernemental de traitement massif (CGTM) afin d'y être conservés dans des conditions optimales (humidité, protection contre l'infiltration d'eau, protection contre le feu, contre le vol, etc.).

<u>Consultation des dossiers papiers déclassés</u>

- L'employé qui détient un accès de requérant au logiciel de traitement des boîtes (EDC) du CGTM, peut le commander lui-même.
- L'employé qui ne détient pas un accès de requérant au logiciel de traitement des boîtes (EDC) du CGTM, doit envoyer sa demande à la conseillère en gestion documentaire.

Quant aux documents technologiques, une procédure de déclassement devra être élaborée en considérant les besoins des employés de la CAI, les obligations légales en matière de protection des renseignements personnels et les outils technologiques disponibles (logiciel de gestion documentaire, lecteur réseau, etc.).

### 7.3 Disposition

La disposition est l'opération qui consiste à détruire ou à conserver les documents qui ont terminé leur stade semi-actif et qui sont devenus inactifs, conformément aux règles de conservation qui y sont rattachées. Les règles de conservation se trouvent dans le calendrier de conservation de la CAI.

En ce qui concerne les documents papier, un processus de disposition devra être élaboré en considérant les besoins des employés de la CAI, les obligations légales en matière de protection des renseignements personnels et les outils technologiques disponibles (logiciel de gestion documentaire, lecteur réseau, etc.). C'est le calendrier de conservation qui détermine si un document doit être détruit de manière confidentielle ou envoyé pour conservation permanente à BAnQ. Si le document est envoyé à BAnQ, il devient la propriété de BAnQ et n'appartient plus à la CAI. Si un employé désire le consulter, il doit en faire la demande auprès de la conseillère en gestion documentaire.

Quant aux documents technologiques, un processus de disposition devra être élaboré en considérant les besoins des employés de la CAI, les obligations légales en matière de protection des renseignements personnels et les outils technologiques disponibles (syGID, lecteur réseau, Sista, etc.). C'est le calendrier de conservation qui détermine si un document doit détruit de manière confidentielle ou envoyé pour conservation permanente à BAnQ. Si le document est envoyé à BAnQ, il devient la propriété de BAnQ et n'appartient plus à la CAI. Si un employé désire le consulter, il doit en faire la demande auprès de la conseillère en gestion documentaire.

## 8. Rôles et responsabilités

La présidente de la Commission d'accès à l'information :

- Approuve la présente Politique.
- Approuve le plan de classification de la CAI.
- Approuve le calendrier de conservation de la CAI.

Le directeur de la direction des affaires institutionnelles, des communications et de la promotion :

- Assume la responsabilité de la gestion documentaire;
- Approuve les documents concernant la gestion documentaire :
    - Calendrier de conservation;
    - Charte de nommage des documents technologiques;
    - Guide de gestion documentaire;
    - Plan de classification;

- Politique organisationnelle de gestion documentaire;
- Procédures;
- Processus.

Les gestionnaires :

- Agissent comme détentrices ou détenteurs responsables des documents produits par leur UA, peu importe le support À ce titre, les gestionnaires sont responsables de la gestion de ces documents pendant toute la durée de leur cycle de vie;
- Appliquent la Politique et les procédures et processus qui en découlent et voient à leur respect au sein de leur UA;
- Assurent la gestion sécuritaire de la documentation contenant de l'information confidentielle, sensible ou essentielle;
- S'assurent que le déclassement annuel des documents semi-actif de leur UA est effectué, peu importe le support;
- Réalisent, pour leur UA et lorsque requis, les activités spécifiques coordonnées par la conseillère en gestion documentaire, telles que :
  - L'approbation et le suivi du déclassement des documents de leur UA, peu importe le support;
  - L'approbation de la disposition des documents de leur UA, peu importe le support;
- S'assurent que le personnel sous leur responsabilité soit formé sur l'utilisation du plan de classification, l'application du calendrier de conservation, l'entreposage des documents papiers, la numérisation (substitution de support), ainsi que l'application de la charte de nommage des documents technologiques.

La conseillère en gestion documentaire :

- Coordonne l'ensemble des activités de gestion documentaire à la CAI;
- Agit comme interlocutrice principale auprès de BAnQ;
- Agit comme interlocutrice principale auprès du CGTM;
- Voit à la conception, au développement, à l'implantation, à la mise à jour et à l'évolution des outils de gestion documentaire :
  - Calendrier de conservation;
  - Charte de nommage des documents technologiques;
  - Guide de gestion documentaire;
  - Plan de classification;
  - Politique organisationnelle de gestion documentaire;

- Procédures;
- Processus.

- Dispense de la formation concernant l'utilisation des différents outils de gestion documentaire, ainsi que sur les grands principes de la gestion documentaire;
- Soutient et conseille les UA de la CAI sur tous les aspects de la gestion documentaire;
- Coordonne le déclassement et la disposition des dossiers.

Le répondant en gestion documentaire :

- Coopère avec la conseillère en gestion documentaire pour :
  - Mettre à jour le plan de classification et le calendrier de conservation;
  - Promouvoir les bonnes pratiques en gestion documentaire auprès des employés qui relèvent de sa direction.
- Agit à titre d'intermédiaire entre les employés qui relèvent de sa direction et la conseillère en gestion documentaire :
  - Les informe des changements apportés aux processus, aux procédures et aux outils de gestion documentaire;
- Enregistre et classe les documents dont il est responsable, selon le plan de classification;
- Effectue le déclassement des documents papier et des documents technologiques qui sont sous sa responsabilité;
- Suit les formations en gestion documentaire dispensées par la conseillère en gestion documentaire;
- Respecte la confidentialité des documents conformément à :
  - La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*;
  - La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*;
  - La *Loi sur la protection des renseignements personnels dans le secteur privé*.

Le personnel de la CAI :

- Enregistre et classe les documents dont il est responsable, selon le plan de classification;
- Suit les formations en gestion documentaire dispensées par la conseillère en gestion documentaire;

- Respecte la confidentialité des documents conformément à :
    - La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*;
    - La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*;
    - La *Loi sur la protection des renseignements personnels dans le secteur privé*.

## 9. Mise à jour

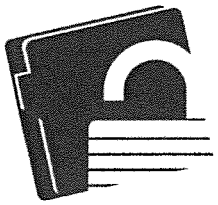
La présente Politique sera révisée tous les trois ans, ainsi que lors de changements importants qui pourraient donner lieu à sa révision.

## 10. Responsable de la Politique

Le directeur de la Direction des affaires institutionnelles, des communications et de la promotion voit à l'application de la présente Politique et à sa mise à jour.

## 11. Approbation

La présente Politique entre en vigueur dès son approbation par la Présidente de la Commission d'accès à l'information.



Commission
d'accès à l'information
du Québec

# CADRE DE GESTION DE LA SÉCURITÉ DE L'INFORMATION

Juin 2016

# Table des matières

# 1 PRÉAMBULE

Le présent cadre de gestion de la sécurité de l'information est un complément à la politique de sécurité de l'information de la Commission d'accès à l'information (la Commission). Il vise à renforcer la gouvernance de la sécurité de l'information à la Commission, par la mise en place d'une structure organisationnelle de la sécurité de l'information et la définition des rôles et responsabilités à tous les niveaux de l'organisation.

Ce cadre est adopté en application de l'article 7 de la *Directive sur la sécurité de l'information gouvernementale* du Conseil du trésor.

# 2 CADRE LÉGAL ET ADMINISTRATIF

Le cadre de gestion est assujetti, entres autres, aux cadres légaux et administratifs suivants :

- la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, chapitre A-2.1);
- le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels* (RLRQ, chapitre A-2.1, r. 02);
- la *Loi concernant le cadre juridique des technologies et l'information* (RLRQ, chapitre C-1.1);
- la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ, chapitre G-1.03);
- la *Directive sur la sécurité de l'information gouvernementale*;
- le *Cadre gouvernemental de gestion de la sécurité de l'information*;
- le *Cadre de gestion des risques et incidents à portée gouvernementale en matière de sécurité de l'information*;
- *l'Approche stratégique gouvernementale 2014-2017 en sécurité de l'information gouvernementale*;
- la *Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics*;
- la *Politique de sécurité de l'information de la Commission*.

# 3 DÉFINITIONS

**Détenteur de l'information :** Un employé désigné par le président, appartenant à la classe d'emploi de niveau cadre ou à une classe d'emploi de niveau supérieur, et dont le rôle est, notamment, de s'assurer de la sécurité de l'information et des ressources qui la sous-tendent, relevant de la responsabilité de son unité administrative.

**Système d'information :** Système constitué des ressources humaines (le personnel), des ressources matérielles (l'équipement) et des procédures permettant d'acquérir, de stocker, de traiter et de diffuser les éléments d'information pertinents pour le fonctionnement d'une entreprise ou d'une organisation. [1]

[1] Source : OQLF – Grand dictionnaire terminologique

# 4 ORGANISATION FONCTIONNELLE DE LA SÉCURITÉ DE L'INFORMATION

Le *Cadre gouvernemental de gestion de la sécurité de l'information* définit l'organisation fonctionnelle de la sécurité de l'information au gouvernement du Québec.

Cette organisation fonctionnelle s'articule autour des deux axes suivants :

1. La structure horizontale, constituée des instances gouvernementales ayant un rôle d'encadrement et de soutien pour les organismes publics;
2. La structure verticale, constituée des organismes publics responsables de la prise en charge des exigences de la sécurité de l'information qui leur incombe.

Voici une description de l'organisation fonctionnelle de la sécurité de l'information au niveau gouvernemental puis au niveau de la Commission.

## 4.1 AU NIVEAU GOUVERNEMENTAL

Le dirigeant principal de l'information appuie le Conseil du trésor dans sa fonction de gouverne de la sécurité de l'information gouvernementale et fournit aux organismes publics les outils et l'assistance leur permettant de prendre en charge les exigences de la sécurité de l'information au sein de leur organisation. Des organismes publics à portée horizontale comme le Centre de services partagés du Québec (CSPQ), le Secrétariat à l'accès à l'information et à la réforme des institutions démocratiques (SAIRID) du Ministère du Conseil exécutif et le Ministère de la Justice du Québec jouent un rôle d'encadrement et de soutien pour les organismes publics. Des instances de concertation comme la table des responsables organisationnels de la sécurité de l'information facilitent les échanges entre les organismes publics.

Le schéma suivant présente une vue d'ensemble de l'organisation fonctionnelle de la sécurité de l'information au gouvernement du Québec.

Pour plus de détails, veuillez consulter le Cadre gouvernemental de gestion de la sécurité de l'information.

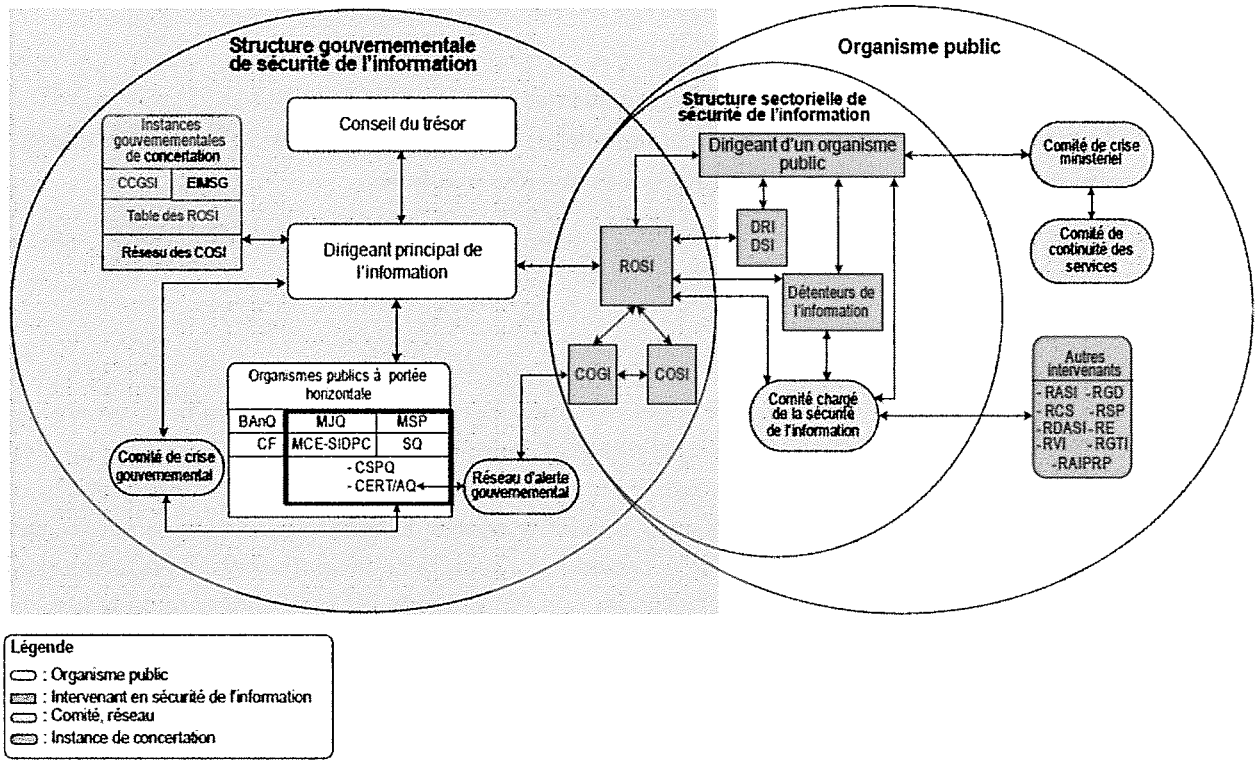



*Figure 1 - Vue d'ensemble de l'organisation fonctionnelle de la sécurité de l'information au gouvernement du Québec*

**Acronymes**

**Organismes publics**

| | |
|---|---|
| BAnQ | Bibliothèque et Archives nationales du Québec |
| CERT/AQ | Équipe de réponse aux incidents de sécurité de l'information de l'administration québécoise |
| CF | Contrôleur des finances |
| CSPQ | Centre de services partagés du Québec |
| MCE – SIDPC | Ministère du Conseil exécutif – Secrétariat aux institutions démocratiques et à la participation citoyenne |
| MJQ | Ministère de la Justice du Québec |
| MSP | Ministère de la Sécurité publique |
| SQ | Sûreté du Québec |

**Instances gouvernementales de concertation**

| | |
|---|---|
| CCGSI | Comité de coordination gouvernementale de la sécurité de l'information |
| EIMSIG | Équipe intégrée sur les menaces à la sécurité de l'information gouvernementale |

**Intervenants en sécurité de l'information**

| | |
|---|---|
| COGI | Coordonnateur organisationnel de gestion des incidents |
| COSI | Conseiller organisationnel en sécurité de l'information |
| DPI | Dirigeant principal de l'information |
| DRI | Dirigeant réseau de l'information |
| DSI | Dirigeant sectoriel de l'information |
| RASI | Responsable de l'architecture de sécurité de l'information |
| RCS | Responsable de la continuité des services |
| RDASI | Responsable du développement ou de l'acquisition des systèmes d'information |
| RE | Responsable de l'éthique |
| RGD | Responsable de la gestion documentaire |
| RGTI | Responsable de la gestion des technologies de l'information |
| ROSI | Responsable organisationnel de la sécurité de l'information |
| RAIPRP | Responsable de l'accès à l'information et de la protection des renseignements personnels |
| RSP | Responsable de la sécurité physique |
| RVI | Responsable de la vérification interne |

## 4.2 Au niveau de la Commission

Le président est le premier responsable de la sécurité de l'information à la Commission. À ce titre, il désigne les intervenants en sécurité de l'information. Les principaux intervenants sont le dirigeant sectoriel de la sécurité de l'information (DSI), le responsable organisationnel de la sécurité de l'information (ROSI), le conseiller organisationnel de la sécurité de l'information (COSI), le coordonnateur organisationnel de gestion des incidents (COGI) et les détenteurs de l'information. Il met également en place un comité chargé de la sécurité de l'information, un comité de crise en réponse aux incidents et un comité de continuité des services. Les autres intervenants comme le responsable de l'éthique ou de la sécurité physique sont également nommés par le président.

Une description détaillée des rôles et responsabilités des intervenants en sécurité de l'information est présentée à la section 5 – Rôles et responsabilités.

Pour un organisme de la taille de la Commission, un même intervenant pourra assumer plus d'un rôle et siéger à plus d'un comité. Pour faciliter les échanges avec les autres organismes publics et par souci de cohérence avec le *Cadre gouvernemental de gestion de la sécurité de l'information,* la Commission a décidé d'attribuer tous les rôles proposés par le cadre gouvernemental.

Les personnes désignées, la composition des comités et la liste des actifs principaux et leurs détenteurs sont présentés à l'Annexe A – Registre d'autorité.

Le schéma suivant présente l'organisation fonctionnelle de la sécurité de l'information au niveau de la Commission.

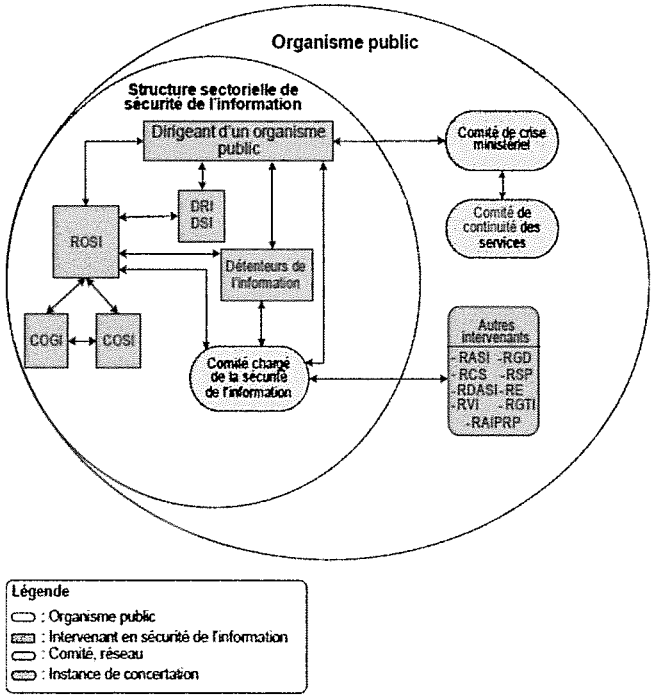



*Figure 2 - Organisation fonctionnelle de la sécurité de l'information au niveau de la Commission*

**Acronymes**

| | |
|---|---|
| **Organismes publics** | |
| BAnQ | Bibliothèque et Archives nationales du Québec |
| CERT/AQ | Équipe de réponse aux incidents de sécurité de l'information de l'administration québécoise |
| CF | Contrôleur des finances |
| CSPQ | Centre de services partagés du Québec |
| MCE – SIDPC | Ministère du Conseil exécutif – Secrétariat aux institutions démocratiques et à la participation citoyenne |
| MJQ | Ministère de la Justice du Québec |
| MSP | Ministère de la Sécurité publique |
| SQ | Sûreté du Québec |
| **Instances gouvernementales de concertation** | |
| CCGSI | Comité de coordination gouvernementale de la sécurité de l'information |
| EIMSIG | Équipe intégrée sur les menaces à la sécurité de l'information gouvernementale |

| | |
|---|---|
| **Intervenants en sécurité de l'information** | |
| COGI | Coordonnateur organisationnel de gestion des incidents |
| COSI | Conseiller organisationnel en sécurité de l'information |
| DPI | Dirigeant principal de l'information |
| DRI | Dirigeant réseau de l'information |
| DSI | Dirigeant sectoriel de l'information |
| RASI | Responsable de l'architecture de sécurité de l'information |
| RCS | Responsable de la continuité des services |
| RDASI | Responsable du développement ou de l'acquisition des systèmes d'information |
| RE | Responsable de l'éthique |
| RGD | Responsable de la gestion documentaire |
| RGTI | Responsable de la gestion des technologies de l'information |
| ROSI | Responsable organisationnel de la sécurité de l'information |
| RAIPRP | Responsable de l'accès à l'information et de la protection des renseignements personnels |
| RSP | Responsable de la sécurité physique |
| RVI | Responsable de la vérification interne |

# 5 RÔLES ET RESPONSABILITÉS

Les responsabilités en matière de sécurité de l'information sont attribuées aux intervenants suivants.

## 5.1 LES PRINCIPAUX INTERVENANTS

### 5.1.1 Le président

Le président est le premier responsable de la sécurité de l'information. À ce titre, il veille au respect du cadre gouvernemental de sécurité de l'information et s'acquitte de ses obligations, telles qu'elles sont édictées dans la *Directive sur la sécurité de l'information gouvernementale*.

À cet effet, il :

a) adopte les orientations stratégiques de la sécurité de l'information à la Commission, la politique, le cadre de gestion, les directives et les plans d's en la matière et en assure la mise en œuvre;
b) approuve les bilans de sécurité de l'information;
c) désigne le responsable organisationnel de la sécurité de l'information, le conseiller organisationnel de la sécurité de l'information, le coordonnateur organisationnel de gestion des incidents ainsi que les détenteurs, et leur attribue les responsabilités définies par le présent cadre de gestion;
d) s'assure de la mise en œuvre des processus officiels de sécurité de l'information permettant, notamment, de veiller à la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents;
e) s'assure de la réalisation périodique d'audits de sécurité de l'information et de tests d'intrusion et de vulnérabilités, conformément aux énoncés de la *Directive sur la sécurité de l'information gouvernementale*, et en dégage les priorités d'action ainsi que les échéanciers afférents;
f) favorise l'utilisation des services communs de sécurité de l'information déterminés par le Conseil du trésor;
g) s'assure que les ententes de service et les contrats conclus avec les prestataires de services, les partenaires et les mandataires comprennent des clauses garantissant le respect des exigences de sécurité de l'information;
h) s'assure de la mise en place d'un programme officiel et continu de formation et de sensibilisation du personnel en matière de sécurité de l'information;
i) approuve et présente aux instances gouvernementales concernées les plans d'action et les bilans requis, conformément aux énoncés de la *Directive sur la sécurité de l'information gouvernementale*.

### 5.1.2 Dirigeant sectoriel de l'information (DSI)

Le dirigeant sectoriel de l'information veille à l'application des règles de gouvernance et de gestion établies en matière de sécurité de l'information.

À cet effet, il :

a) assure le suivi de la mise en œuvre des recommandations émises par le Conseil du trésor ou par le dirigeant principal de l'information;
b) examine les plans d'action de la Commission et propose si nécessaire des modifications à y apporter;
c) contribue, conjointement avec le dirigeant principal de l'information et le CERT/AQ, à la définition et à la mise en œuvre du processus de gestion des incidents à portée gouvernementale.

### 5.1.3 Responsable organisationnel de la sécurité de l'information (ROSI)

Le responsable organisationnel de la sécurité de l'information représente la Commission auprès du dirigeant principal de l'information, en matière de sécurité de l'information.

À cet égard, il :

a) joue le rôle de porte-parole du dirigeant principal de l'information en matière de sécurité de l'information et lui fait part de ses réalisations;
b) transmet au président de la Commission les orientations et les priorités d'intervention gouvernementales et s'assure de leur mise en œuvre;
c) soumet aux fins de consultation, au comité chargé de la sécurité de l'information, soit le comité sur l'accès à l'information et sur la protection des renseignements personnels et la sécurité de l'information (AIPRP-SI), les orientations, les politiques, les directives, les cadres de gestion, les priorités d'actions, les éléments de reddition de comptes ainsi que tout événement ayant mis ou qui aurait pu mettre en péril la sécurité de l'information;
d) assure, en collaboration avec le comité AIPRP-SI, la coordination et la cohérence des actions de sécurité de l'information menées au sein de la Commission par d'autres intervenants dont, notamment, le responsable de l'accès à l'information et de la protection des renseignements personnels, les détenteurs de l'information ainsi que les unités responsables des ressources informationnelles, de la gestion documentaire, de la sécurité physique et de l'éthique;
e) s'assure de la contribution de la Commission au processus de gestion des risques et des incidents de sécurité de l'information à portée gouvernementale;
f) déclare au dirigeant principal de l'information les risques de sécurité de l'information à portée gouvernementale;
g) déclare au CERT/AQ les incidents de sécurité de l'information à portée gouvernementale;
h) définit et met en œuvre, en collaboration avec le comité AIPRP-SI, les processus officiels de sécurité de l'information tels que la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents;
i) coordonne l'élaboration et la mise en œuvre d'un programme continu de formation et de sensibilisation en matière de sécurité de l'information;
j) participe aux tables de coordination et de concertation gouvernementales en matière de sécurité de l'information;
k) participe à des comités interministériels et représente la Commission en matière de sécurité de l'information.

### 5.1.4 Le conseiller organisationnel en sécurité de l'information (COSI)

Le conseiller organisationnel en sécurité de l'information apporte, au niveau tactique, son soutien au ROSI, notamment en ce qui concerne la mise en œuvre des mesures de sécurité et la mise en place des processus officiels de sécurité de l'information.

À cet égard, il :

a) met en œuvre les orientations internes découlant des directives gouvernementales, des politiques internes et des pratiques généralement admises à cet égard;
b) produit les bilans et les plans d'action de sécurité de l'information de la Commission;
c) s'assure, en collaboration avec la Direction des affaires juridiques, de l'intégration de dispositions garantissant le respect des exigences de sécurité de l'information dans le cadre des ententes de service et des contrats;
d) assiste les détenteurs dans la catégorisation de l'information relevant de leur responsabilité et dans la réalisation des analyses de risques de sécurité de l'information;
e) élabore et met en œuvre le programme de formation et de sensibilisation en matière de sécurité de l'information;
f) tient à jour le registre d'autorité de la sécurité de l'information;
g) participe au réseau des conseillers organisationnels en sécurité de l'information;
h) propose au ROSI des orientations, des plans d'action et des bilans;
i) assure la coordination et la réalisation de projets de sécurité de l'information.

### 5.1.5 Le coordonnateur organisationnel de gestion des incidents (COGI)

Le coordonnateur organisationnel de gestion des incidents participe activement au réseau d'alerte gouvernemental et collabore étroitement avec le ROSI et le COSI.

Il a notamment pour responsabilités :

a) de contribuer à la mise en place du processus sectoriel de gestion des incidents de sécurité de l'information et du processus gouvernemental de gestion des incidents;
b) de tenir à jour le registre des incidents ayant pu mettre en péril la sécurité de l'information, de documenter ces incidents et d'en tenir informés le ROSI et le comité chargé de la sécurité de l'information, soit le comité AIPRP-SI;
c) de contribuer à l'analyse des risques de sécurité de l'information, de déterminer les menaces et les situations de vulnérabilité et de mettre en œuvre les solutions appropriées;
d) d'élaborer et de tenir à jour les guides portant sur la sécurité opérationnelle des systèmes et des réseaux de télécommunication.

## 5.2 LES AUTRES INTERVENANTS

### 5.2.1 Détenteurs de l'information

Les détenteurs de l'information désignés par le président sont notamment chargés :

a) de catégoriser l'information relevant de leur responsabilité en matière de disponibilité, d'intégrité et de confidentialité;
b) d'agir comme maîtres d'œuvre des analyses de risques et de s'assurer de la prise en charge des risques résiduels;

c) de participer à l'élaboration des orientations stratégiques, des politiques, des directives, des cadres de gestion, des guides, des plans d'action et des bilans;
d) de veiller à la mise en place et à l'application des mesures de sécurité de l'information, y compris celles liées au respect des exigences légales de protection des renseignements personnels;
e) de s'assurer de l'adéquation des mesures de sécurité de l'information en vigueur par rapport aux risques encourus.

### 5.2.2 Le gestionnaire

Le gestionnaire est responsable de la mise en œuvre, auprès du personnel relevant de son autorité, des dispositions de la politique de sécurité de l'information.

Il doit principalement :

a) informer son personnel des dispositions de la politique sur la sécurité de l'information et de toute directive, de tout standard et de toute procédure en vigueur en matière de sécurité de l'information, ainsi que des modalités liées à leur mise en œuvre, et le sensibiliser à la nécessité de s'y conformer;
b) s'assurer que les actifs informationnels mis à la disposition de son personnel sont utilisés en conformité avec les principes généraux et les exigences de la politique de sécurité;
c) aviser le ROSI dans les meilleurs délais, lorsqu'il soupçonne une violation des règles de sécurité ou toute anomalie pouvant nuire à la protection des actifs informationnels de la Commission;
d) s'assurer, en collaboration avec la Direction des affaires juridiques, que la sécurité de l'information est prise en compte dans tout contrat de service attribué par son unité administrative et voir à ce que tout consultant, partenaire ou fournisseur s'engagent à respecter et respectent les règles de sécurité de l'information de la Commission.

### 5.2.3 Les utilisateurs

Les utilisateurs jouent un rôle important dans la protection des actifs informationnels de la Commission.

À cette fin, les utilisateurs doivent :

a) prendre connaissance de la politique de sécurité de l'information de la Commission, des directives, des procédures et autres lignes de conduite qui seront prises par la suite par la Commission et s'y conformer;
b) utiliser les actifs informationnels mis à leur disposition en se limitant aux fins auxquelles ils ont été autorisés;
c) éviter tout comportement pouvant porter atteinte aux diverses mesures de sécurité mises en place par la Commission pour assurer la sécurité des actifs informationnels tels que la sécurité des lieux ou des équipements physiques et électroniques;
d) signaler immédiatement à son supérieur tout acte dont il a connaissance, susceptible de constituer une violation réelle ou présumée des règles de sécurité ainsi que toute anomalie pouvant nuire à la protection des actifs informationnels de la Commission;
e) remettre, lorsqu'ils quittent la Commission, les différents actifs informationnels mis à leur disposition par la Commission tels que les cartes d'identité et d'accès aux locaux, les équipements électroniques et de téléphonie.

### 5.2.4 Responsable de l'architecture de sécurité de l'information

Le responsable de l'architecture de sécurité de l'information doit, notamment :

a) concevoir et mettre en œuvre l'architecture décrivant la fonction, la structure et les interrelations des composantes de sécurité de l'information;
b) arrimer les solutions retenues aux processus organisationnels de sécurité de l'information;
c) participer à la conception et à l'évaluation des composantes de sécurité de l'information des solutions d'affaires, élaborées ou acquises par la Commission.

### 5.2.5 Responsable de la gestion des technologies de l'information

Le responsable de la gestion des technologies de l'information doit, notamment :

a) contribuer à l'élaboration et à la mise en œuvre de directives contribuant à assurer la sécurité de l'information numérique;
b) mettre en œuvre les mesures permettant d'assurer la sécurité de l'information numérique détenue par la Commission, dont les plans de reprise informatique en cas de sinistre;
c) mettre en place, en collaboration avec le comité AIPRP-SI, un cadre normatif de développement assurant la prise en charge des exigences de sécurité de l'information, y compris celles liées au respect des exigences légales de protection des renseignements personnels, lors de la réalisation d'un projet de développement ou lors de l'acquisition d'un système d'information.

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

Le responsable de l'accès à l'information et de la protection des renseignements personnels veille au respect de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (chapitre A-2.1).

À ce titre, il :

a) communique au ROSI, ainsi qu'aux membres du comité AIPRP-SI, les problématiques et les préoccupations de sécurité en matière de protection des renseignements personnels ou à caractère sensible;
b) contribue à assurer la cohérence et l'harmonisation des interventions entre la sécurité de l'information, l'accès aux documents et la protection des renseignements personnels, y compris lors de la mise en œuvre du processus de gestion des risques et des incidents de sécurité de l'information.

### 5.2.7 Responsable de la gestion documentaire

Le responsable de la gestion documentaire doit, notamment :

a) collaborer à la conception des systèmes informatiques, administratifs ou autres et s'assurer qu'à toutes les étapes du cycle de vie de l'information, ces systèmes ont les qualités nécessaires à une saine gestion des connaissances et du patrimoine informationnel, à la préservation des preuves et au respect des lois;
b) collaborer étroitement avec les détenteurs de l'information, le responsable ou le conseiller organisationnel en sécurité de l'information, en vue de déterminer, de gérer, de coordonner et de mettre en œuvre des mesures de sécurité de l'information, indépendamment de son support.

### 5.2.8 Responsable du développement ou de l'acquisition de systèmes d'information

Le responsable du développement ou de l'acquisition de systèmes d'information conçoit, réalise et documente les fonctionnalités de sécurité de l'information, y compris celles liées au respect des exigences légales de protection des renseignements personnels, à intégrer aux systèmes d'information et s'assure de leur bon fonctionnement.

### 5.2.9 Responsable de la continuité des services

Le responsable de la continuité des services assure la gestion et la coordination du plan de continuité des services de la Commission.

Plus particulièrement, il :

a) coordonne l'élaboration du plan de continuité des services, veille à sa mise en œuvre et en assure la mise à jour;
b) assure la planification et la coordination des tests initiaux et récurrents.

### 5.2.10 Responsable de la sécurité physique

Le responsable de la sécurité physique met en place les mesures de protection physique des locaux et de sécurisation de leurs accès, notamment lorsqu'ils abritent des systèmes et des installations technologiques stratégiques ou essentielles ou des supports de l'information confidentielle.

Plus particulièrement, le responsable de la sécurité physique :

a) conçoit et met en œuvre les mesures de protection physique des biens contre les sinistres, les pertes, les dommages, le vol ainsi que l'interruption des activités de la Commission;
b) s'assure de la mise au rebut sécuritaire des supports de l'information;
c) élabore et met en œuvre des directives, des guides et des procédures propres à son domaine d'intervention.

### 5.2.11 Responsable de la vérification interne

Le responsable de la vérification interne joue un rôle-clé dans la reddition de comptes en matière de sécurité de l'information, plus particulièrement au regard de la détermination, de l'évaluation et de la gestion des risques d'atteinte à la sécurité de l'information.

À ce titre, il évalue, examine ou vérifie, notamment :

a) l'application, la validité et l'efficacité des règles, des mesures administratives et des moyens technologiques en matière de sécurité de l'information élaborés et mis en œuvre;
b) l'adéquation de l'intégration de la sécurité de l'information dans les processus d'affaires.

### 5.2.12 Responsable de l'éthique

Le responsable de l'éthique veille à l'intégration de l'éthique dans les processus de gestion de la sécurité de l'information, afin d'assurer la régulation des conduites et la responsabilisation individuelle.

## 5.3 LES COMITÉS

### 5.3.1 Comité sur l'accès à l'information et sur la protection des renseignements personnels et la sécurité de l'information (AIPRP-SI)

Ce comité est présidé par le président. Il est composé, notamment, du responsable de l'accès aux documents et de la protection des renseignements personnels, du ROSI, des détenteurs de l'information ainsi que des unités responsables des ressources informationnelles, de la vérification interne, de la gestion documentaire, de la sécurité physique et de l'éthique.

En plus de son rôle en matière d'accès à l'information et de protection des renseignements personnels, ce comité est la principale instance sectorielle de concertation en matière de sécurité de l'information.

Plus particulièrement, en matière de sécurité de l'information, le comité, sous l'autorité du dirigeant sectoriel de l'information :

a) examine et formule des recommandations concernant les orientations, les politiques, les directives, les cadres de gestion, les plans d'action et les bilans de la Commission, ainsi que toute proposition d'action ou état d'avancement de projets en sécurité de l'information;
b) analyse et formule des recommandations concernant les événements ayant mis ou qui auraient pu mettre en péril la sécurité de l'information de la Commission.

### 5.3.2 Comité de continuité des services

Le comité de continuité des services est principalement composé du responsable de la continuité des services, des détenteurs de l'information, du ROSI, du COSI et du COGI.

Il a pour rôle, notamment :

a) de procéder à l'évaluation des dommages;
b) de recommander au comité de crise l'adoption d'une déclaration de sinistre;
c) d'assurer la mise en œuvre du plan de mobilisation;
d) d'assurer la coordination avec les intervenants externes.

Ce comité peut s'adjoindre toute autre personne en mesure de lui assurer le soutien adéquat dans ses prises de décision. Il est présidé par le responsable de la continuité des services ou son représentant.

### 5.3.3 Comité de crise

En cas d'incident critique de sécurité de l'information, le comité de crise est le groupe décisionnel appelé à intervenir, notamment lorsque les tentatives de rétablissement des activités n'ont pas apporté les résultats escomptés ou qu'aucune mesure palliative n'a pu assurer la continuité ou la reprise rapide des services.

À ce titre, il a pour rôle, principalement :

a) d'autoriser la mise en œuvre de stratégies permettant d'assurer la prise en charge des incidents critiques de sécurité de l'information;
b) d'adopter la déclaration de sinistre proposée par le responsable de la continuité des services et d'approuver les budgets spéciaux correspondants;
c) de décider du déploiement ou non des plans de continuité des services;
d) de proposer des orientations à suivre ou des actions à prendre en cas de sinistre;
e) de formuler des recommandations concernant le délestage, en totalité ou en partie, des activités de la Commission;
f) de communiquer avec les médias.

Le noyau permanent de ce comité est composé de représentants de la haute direction, du ROSI, du responsable de la protection des renseignements personnels, du responsable de la sécurité physique et du responsable de la continuité des services. Ce comité peut s'adjoindre toute autre personne en mesure de lui assurer le soutien adéquat dans ses prises de décision. Citons, à titre d'exemple, les détenteurs de l'information ou les conseillers pour les volets juridique, technologique et de communication avec les médias et les ressources humaines.

Le comité de crise est présidé par le président.

# 6 DISPOSITIONS FINALES

a) le présent cadre de gestion entre en vigueur à la date de son approbation par le président;
b) ce cadre de gestion est complémentaire à la politique de sécurité de l'information de la Commission.

[redacted]

**Jean Chartier, président**

23 juin 2016.

**Date**

# ANNEXE A – REGISTRE D'AUTORITÉ

| Désignation des intervenants en sécurité de l'information | |
|---|---|
| Dirigeant sectoriel de l'information (DSI) | Rémi Bédard |
| Responsable organisationnel de la sécurité de l'information (ROSI) | Rémi Bédard |
| Conseiller organisationnel de la sécurité de l'information (COSI) | Jean-Pierre Philibert |
| Coordonnateur organisationnel de gestion des incidents (COGI) | Jean-Pierre Philibert |
| Responsable de l'architecture de sécurité de l'information (RASI) | Jean-Pierre Philibert |
| Responsable de la gestion des technologies de l'information | Jean-Pierre Philibert |
| Responsable de l'accès à l'information et de la protection des renseignements personnels | Claire-Élaine Audet |
| Responsable de la gestion documentaire | Miguel Poiré |
| Responsable du développement ou de l'acquisition de systèmes d'information | Jean-Pierre Philibert |
| Responsable de la continuité des services | Jean-Pierre Philibert |
| Responsable de la sécurité physique | Pierre Jobin |
| Responsable de la vérification interne | À définir |
| Responsable de l'éthique | Sophie Giroux-Blanchet |

| Composition des comités en sécurité de l'information | |
|---|---|
| Comité sur l'accès à l'information et sur la protection des renseignements personnels et la sécurité de l'information (AIPRP-SI) | Le comité AIPRP-SI est présidé par le président. Il est composé, notamment, du responsable de l'accès aux documents et de la protection des renseignements personnels, du ROSI, des détenteurs de l'information ainsi que des unités responsables des ressources informationnelles, de la vérification interne, de la gestion documentaire, de la sécurité physique et de l'éthique.<br>Ce comité peut s'adjoindre toute autre personne en mesure de lui assurer le soutien adéquat dans ses prises de décision. |
| Comité de continuité des services | Le comité de continuité des services se tient, au besoin, lors d'une séance spéciale du comité de direction.<br>Il est composé des membres du comité de direction, du responsable de la continuité des services, du COSI et du COGI.<br>Ce comité peut s'adjoindre toute autre personne en mesure de lui assurer le soutien adéquat dans ses prises de décision. |
| Comité de crise | Le comité de crise se tient, au besoin, lors d'une séance spéciale du comité de direction.<br>Il est composé des membres du comité de direction, du responsable de la sécurité physique et du responsable de la continuité des services.<br>Ce comité peut s'adjoindre toute autre personne en mesure de lui assurer le soutien adéquat dans ses prises de décision. |

| Actifs informationnels et détenteurs[2] | | |
|---|---|---|
| Actif | Description | Détenteur |
| Dossiers juridictionnels | Les dossiers de mission de la section juridictionnelle | Secrétaire général |
| Dossiers de recours devant les tribunaux civils | | Directeur des affaires juridiques |
| Dossiers de médiation | | Directeur des affaires juridiques |
| Dossiers administratifs de la Direction des affaires juridiques | | Directeur des affaires juridiques |
| Dossiers du Secrétariat général | Les dossiers de mission du secrétariat général (ex. : rapport quinquennal) | Secrétaire général |
| Dossiers administratifs du Secrétariat général | | Secrétaire général |
| Dossiers de surveillance | Les dossiers de mission de la section de surveillance | Secrétaire général |
| Dossiers administratifs de la Direction de la surveillance | | Directeur de la surveillance |
| Dossiers en ressources humaines | | Directeur de l'administration |
| Dossiers en ressources informationnelles | | Directeur de l'administration |
| Dossiers en ressources financières | | Directeur de l'administration |
| Dossiers en ressources matérielles | | Directeur de l'administration |
| Dossiers en communication | | Directeur de la surveillance |
| Fichier de traitement des demandes médiatiques | | Directeur de la surveillance |
| Système de gestion des appels aux préposées (GAP) | | Directeur de la surveillance |
| Fichier des demandes d'accès | | Président |
| Fichier de traitement des plaintes | | Président |
| Dossiers de la Présidence | | Président |

[2] À revoir lors de la catégorisation des actifs informationnels de la Commission.

Commission
d'accès à l'information
du Québec

# DIRECTIVE SUR L'UTILISATION DES TECHNOLOGIES DE L'INFORMATION

Août 2022

# Table des matières

# 1. OBJECTIFS

La présente directive est adoptée conformément à la politique et au cadre de gestion de la sécurité de l'information de la Commission d'accès à l'information (la Commission) qui sont entrés en vigueur le 23 juin 2016.

Ses objectifs sont :

a) d'établir les règles d'utilisation des outils informatiques à la Commission d'accès à l'information;

b) de préserver la disponibilité, l'intégrité et la confidentialité des actifs informationnels de la Commission et assurer la dimension éthique des communications reliant la Commission aux citoyens et aux organisations publiques et privées;

c) d'assurer le respect de toute législation à l'égard de l'usage et du traitement de l'information et de l'utilisation des technologies de l'information.

Pour plus d'information sur les composantes du cadre normatif de sécurité de l'information, reportez-vous à l'annexe C de la politique de sécurité de l'information de la Commission.

# 2. CHAMPS D'APPLICATION

La présente directive s'applique à tous les utilisateurs des actifs informationnels et des outils informatiques de la Commission.

# 3. DÉFINITIONS

**Actif informationnel**

Une information, quel que soit son canal de communication ou son support (papier, électronique, etc.), un système ou un support d'information, une technologie de l'information, une installation ou un ensemble de ces éléments, acquis ou constitués par une organisation.

**Outil informatique**

Serveurs, ordinateurs, mini-ordinateurs, micro-ordinateurs, postes de travail informatisés et leurs unités ou accessoires périphériques de lecture, d'emmagasinage, de reproduction, d'impression, de transmission, de réception et de traitement de l'information. Tout équipement de télécommunication dont les téléphones intelligents, les logiciels et le système de courrier électronique placé sur un équipement ou sur un média informatique appartenant à la Commission ou ne lui appartenant pas, mais utilisé dans ses locaux, peu importe leur localisation.

**Système d'information**

Système constitué des ressources humaines, des ressources matérielles et des procédures permettant d'acquérir, de stocker, de traiter et de diffuser les éléments d'information pertinents pour le fonctionnement d'une entreprise ou d'une organisation.

**Télétravail**

Forme d'organisation du travail qui consiste pour un utilisateur à effectuer sa prestation de travail en dehors des locaux de la Commission, généralement à partir du domicile, en utilisant les technologies de l'information et de la communication.

**Télétravailleur**

Employé qui effectue du télétravail.

**Lieu de télétravail**

Endroit où le président autorise l'employé à exercer ses fonctions qu'il aurait autrement exécutées dans les locaux de l'employeur.

**Utilisateur**

Toute personne, physique ou morale, qui est dûment autorisée à accéder aux actifs informationnels de la Commission ou qui les utilise.

**Clavardage**

Activité permettant à un internaute d'avoir une conversation écrite, interactive et en temps réel avec d'autres internautes par claviers interposés.

**Droit d'utilisation**

Autorisation accordée à une personne définissant l'usage qu'elle peut faire des actifs informationnels et des outils informatiques.

**Internet**

Réseau informatique mondial constitué d'un ensemble de réseaux nationaux, régionaux et privés, qui sont reliés par le protocole de communication TCP/IP et qui coopèrent dans le but d'offrir une interface unique à leurs utilisateurs.

**Intranet**

Réseau informatique utilisé à l'intérieur d'une entreprise ou de toute autre entité organisationnelle qui utilise les mêmes protocoles qu'Internet (TCP/IP, HTTP, SMTP, IMAP, etc.). Parfois, le terme se réfère uniquement au site Web interne de l'organisation, mais c'est souvent une partie bien plus large de l'infrastructure informatique d'une organisation.

Propriétaire d'équipe

Le gestionnaire ou la personne désignée d'une unité administrative pour gérer les accès aux actifs informationnels de l'unité.

# 4. RÔLES ET RESPONSABILITÉS

| | |
|---|---|
| **Le président** | Adopte la présente directive et est responsable de son application. Approuve l'application de mesures de contrôle et de surveillance du contenu et de l'utilisation des actifs et des outils informatiques de la Commission et de sanctions. |
| **Le chef de la sécurité de l'information organisationnelle (CSIOCSIO)** | Assure la mise en œuvre de la présente directive, assiste le président lors des vérifications de l'utilisation et assure la gestion de l'accès aux actifs informationnels et aux outils informatiques. |
| **Le responsable de la protection des renseignements personnels** | Supervise le COSI lors de l'application de mesures de contrôle du contenu et de l'utilisation des actifs informationnels et des outils informatiques de la Commission. |
| **Le responsable de l'éthique** | Exerce, au besoin, un rôle-conseil auprès du président dans l'application de mesures de vérification ponctuelle du contenu et de l'utilisation des actifs informationnels et des outils informatiques de la Commission par un utilisateur. |
| **Le coordonnateur organisationnel en sécurité de l'information (COSI)** | Informe les utilisateurs de l'existence de la présente directive et en assure la mise à jour. Applique les mesures de contrôle et de surveillance du contenu et de l'utilisation des actifs informationnels et des outils informatiques. |
| **Le propriétaire d'équipe** | Gère les accès aux actifs informationnels appartenant à son équipe de façon à préserver la disponibilité, l'intégrité et la confidentialité. À cette fin, il accorde uniquement les accès nécessaires aux fonctions du demandeur et retire les accès dès qu'ils ne sont plus requis. |
| **Le gestionnaire** | Informe son personnel des dispositions de la directive ainsi que des modalités liées à leur mise en œuvre et les sensibilise à la nécessité de s'y conformer. Informe le CSIO dans les meilleurs délais, lorsqu'il soupçonne une violation des règles de cette directive. |
| **L'utilisateur** | Prend connaissance de la présente directive et s'y conforme. Utilise les actifs informationnels et les outils informatiques mis à sa disposition en se limitant aux fins auxquelles leur utilisation a été autorisée. Évite tout comportement allant à l'encontre des règles de la présente directive. Remet, lorsqu'il quitte la Commission, les différents actifs informationnels et les outils informatiques mis à sa disposition par la Commission. |

## 5. ÉNONCÉS GÉNÉRAUX

a) L'utilisation des actifs informationnels et des outils informatiques de la Commission est un privilège et non un droit. Il peut être révoqué en tout temps à tous les utilisateurs qui ne se conforment pas à la présente directive;

b) Toute information stockée ou consignée sur les outils informatiques de la Commission au moyen d'un courriel, d'un collecticiel, des services d'internet ou par tout autre moyen est réputée constituer une information à laquelle la Commission peut accéder;

c) La Commission se réserve le droit, sur demande du président, de contrôler le contenu et l'utilisation de ses actifs informationnels et de ses outils informatiques lorsqu'elle a des motifs sérieux de croire qu'un utilisateur n'agit pas conformément aux règles de la présente directive;

d) L'utilisation des outils informatiques de la Commission rend possible son identification ou l'identification du gouvernement du Québec par un interlocuteur externe. L'utilisateur doit en tenir compte;

e) L'utilisateur signale immédiatement à son gestionnaire tout acte dont il a connaissance, qui est susceptible de constituer une violation réelle ou présumée des règles.

## 6. CONDITIONS D'UTILISATION GÉNÉRALES

a) L'utilisation des actifs informationnels et des outils informatiques de la Commission à des fins illicites, illégales, lucratives, commerciales, de publicité, de propagande, de harcèlement, de diffusion de propos diffamatoires, haineux, offensants, perturbants, dénigrants ou de contenu sexuellement explicite ou obscène ou incompatible avec la mission ou l'image de la Commission est strictement interdite;

b) L'utilisateur doit prendre les moyens disponibles pour voir à la sécurité de l'information et la protection des renseignements auxquels il a accès conformément aux lois, à la réglementation et aux directives en vigueur[1] lors de l'utilisation des actifs informationnels et des outils informatiques de la Commission. Ceci est particulièrement important lors de l'envoi de courriel, de partage de documents et de l'utilisation d'outils de visioconférence.

[1] Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ., c. A-2.1);
Loi concernant le cadre juridique des technologies et l'information (RLRQ, c. C-1.1);
Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, chapitre G-1.03);
Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics;
Politique et cadre de gestion de la sécurité de l'information de la Commission d'accès à l'information;
Directive sur la sécurité de l'information gouvernementale.

c) L'utilisateur a l'obligation de respecter les mesures de sécurité, notamment et non limitativement les filtres Internet, les coupe-feux et l'authentification multifacteur, mis en place à la Commission;

d) L'utilisateur doit prendre les précautions nécessaires pour se prémunir du vol de ses appareils, par exemple, il ne doit pas les laisser dans la voiture;

e) L'utilisateur a l'obligation de s'identifier clairement lors de toute utilisation des actifs informationnels et des outils informatiques de la Commission en utilisant les identifiants qui lui ont été alloués;

f) L'utilisateur ne doit pas donner ses identifiants ni ses mots de passe et est responsable de toute forme de communication qui pourrait être effectuée avec ceux-ci dans le cas contraire;

g) Les actifs informationnels et les outils informatiques de la Commission sont mis à la disposition des utilisateurs pour la réalisation de leurs fonctions professionnelles et demeurent la propriété de la Commission. Un usage à des fins personnelles est admis dans la mesure où il ne réduit pas la sécurité des actifs informationnels, la productivité de l'utilisateur et ne nuit pas aux intérêts ou à l'image de la Commission;

h) Le stockage de documents (photos, vidéos, courriels, etc.) personnels est permis. Toutefois, il ne doit pas avoir pour effet de limiter l'accès, d'interrompre le fonctionnement ou de diminuer le rendement des actifs informationnels et des outils informatiques de la Commission ou d'entraîner des coûts additionnels;

i) L'enregistrement de documents contenants des renseignements personnels sur un support mobile (ex. : clé USB) est interdit à moins que l'utilisateur utilise une clé USB cryptée et après avoir reçu l'autorisation de son gestionnaire;

j) L'utilisateur ne peut utiliser les actifs informationnels et les outils informatiques de la Commission pour expédier des messages destinés à tous les utilisateurs sur des sujets qui ne sont pas d'ordre professionnel;

k) L'utilisateur ne doit pas permettre l'utilisation des appareils de la Commission par qui que ce soit;

l) Le télétravailleur doit accéder aux documents appartenant à la Commission en n'utilisant que les outils informatiques mis à sa disposition. Il ne doit pas apporter de documents en version papier à son lieu de télétravail, à moins que ceux-ci ne soient pas accessibles via les outils informatiques mis à sa disposition. S'il doit le faire, il doit conserver les documents contenant des renseignements confidentiels reliés à son travail dans un bureau ou un classeur verrouillé. De plus, il doit uniquement en disposer aux endroits prévus à cette fin dans les locaux de l'employeur.

m) Le télétravailleur ne doit pas imprimer de documents appartenant à la Commission à son lieu de télétravail à moins que les outils informatiques que la Commission met à sa disposition ne lui permettent pas d'effectuer sa tâche autrement. S'il doit le faire, il doit conserver les

documents contenant des renseignements confidentiels reliés à son travail dans un bureau ou un classeur verrouillé. De plus, il doit uniquement en disposer aux endroits prévus à cette fin dans les locaux de l'employeur.

n) Chaque consultation que l'utilisateur fait sur Internet et chaque message électronique qu'il transmet identifie et associe la Commission et le gouvernement du Québec à cette consultation ou cette transmission. Ainsi, l'utilisateur doit protéger l'image et la réputation de la Commission et du gouvernement. Ses communications doivent être empreintes de courtoisie, de respect et de civisme et être faites dans un langage adéquat.

# 7. CONDITIONS D'UTILISATION SPÉCIFIQUES

## 7.1. POSTE DE TRAVAIL (FIXE OU PORTABLE)

a) L'utilisateur doit verrouiller son poste de travail à chaque fois qu'il le quitte;

b) L'utilisateur doit arrêter (éteindre) son poste de travail à la fin de chaque journée de travail afin d'éviter des problèmes de redémarrage;

c) L'utilisateur doit, lorsqu'il reçoit une notification à cet effet, procéder à la mise à jour de son poste de travail dans les meilleurs délais;

Lorsque les mises à jour requièrent l'assistance d'un administrateur, il communique avec l'équipe TI.

d) L'utilisateur ne doit pas télécharger, partager ou copier des logiciels, des fichiers entraînant l'installation d'un programme (.exe, .bat, .com, etc.), des outils ayant pour tâche d'analyser, de traduire et d'exécuter les programmes (.js, .vbs, etc.) ou des fichiers non reliés aux applications bureautiques autorisées, des économiseurs d'écran, des jeux ou des images (à l'exception des photos personnelles);

e) L'utilisateur ne doit pas enregistrer de documents ou de fichiers d'ordre professionnel dans One Drive. Il doit obligatoirement enregistrer ces documents dans un des canaux qui lui sont accessibles par Microsoft Teams ou directement dans Sharepoint.

f) L'installation de logiciels autres que ceux installés par la Commission de même que l'utilisation d'applications autres que celles développées par Microsoft elle-même sans le consentement du CSIO est interdite. L'installation ou l'utilisation de logiciels sans licence ou sur un nombre de postes plus élevés que le nombre de licences détenues par la Commission d'accès à l'Information est également interdite. La reproduction de logiciels n'est autorisée qu'à des fins de copies de sauvegarde, et ce, en conformité avec les normes de la licence d'utilisation les régissant. Quant à l'utilisation d'application développées par des tiers, elle peut comporter des enjeux de sécurité;

g) Il est interdit d'installer et d'utiliser un logiciel acquis pour un usage externe à la Commission sans que la licence ou le droit de propriété n'ait été transféré au nom de la Commission.

## 7.2. TÉLÉPHONES INTELLIGENTS)

a) Tout téléphone intelligent doit être protégé par un mot de passe et un mécanisme de chiffrement;

b) L'utilisateur doit verrouiller son téléphone intelligent dès qu'il cesse de l'utiliser et ne pas le laisser sans surveillance;

c) Le partage de connexion à partir d'un téléphone intelligent appartenant à la Commission vers un autre appareil est interdit;

d) À partir des rapports de consommation mensuelle de téléphonie mobile transmis à son gestionnaire par la direction de l'administration, l'utilisateur rembourse à la Commission tout frais découlant de l'utilisation de services non-inclus dans le forfait standard et lié à une utilisation à des fins personnelles.

## 7.3. SERVICES INTERNET

a) L'accès et la consultation de sites Internet qui véhiculent des messages obscènes, haineux, racistes, diffamatoires, harcelants ou violents ainsi qu'à des sites contenant du matériel érotique ou pornographique sont interdits. Il en va de même pour tout envoi et toute réception de courriels (autres que ceux non sollicités) qui auraient une semblable connotation;

b) La participation à des activités de piratage (musique, jeux, logiciels, etc.), des jeux de hasard, des paris, des concours ou des groupes de discussion ou de clavardage, sauf si ces groupes portent sur des sujets d'ordre professionnel et que la participation est autorisée par le gestionnaire, est interdite;

c) L'utilisation de logiciels ou de services de partage de fichiers (Torrent, Kaza, Usenet, Dropbox, etc.) est interdite;

d) L'utilisation de services Internet doit se faire, en priorité, par câble. À défaut d'avoir accès à un réseau par câble, l'utilisation de réseaux sans-fil sécurisés (accessibles avec mot de passe) est possible. Toutefois, l'utilisateur doit redoubler de vigilance. L'utilisation de réseaux sans-fil non-sécurisés (accessibles sans mot de passe) est à proscrire;

e) La Commission se réserve le droit de mettre en place des mécanismes de filtrage afin de limiter l'accès aux sites Internet dont le contenu est incompatible avec la mission de la Commission ou avec les règles de la présente directive;

f) L'écoute d'émissions de radio ou de télévision de même que l'écoute de musique diffusées numériquement sur Internet (streaming) pendant les heures de travail est interdite, sauf pour les cas reliés à l'exercice des fonctions de l'utilisateur et que l'écoute est autorisée par le gestionnaire;

L'écoute de telles émissions sur les téléphones intelligents de la Commission est interdite en tout temps sauf pour les cas reliés à l'exercice des fonctions de l'utilisateur et que l'écoute est autorisée par le gestionnaire. À moins qu'il soit impossible d'utiliser un réseau WiFi pour le faire, la personne autorisée ne doit pas utiliser le réseau cellulaire. L'appareil devrait même être déconnecté du réseau cellulaire pendant l'écoute.

### 7.4. MESSAGERIE ÉLECTRONIQUE ET COURRIEL

a) L'utilisateur doit faire preuve de vigilance lors de l'ouverture d'un courriel dont il ignore la provenance, dont l'expéditeur est inconnu ou dont il doute de l'authenticité. Il s'assure de communiquer avec le COSI avant de cliquer sur un lien Internet ou sur une pièce jointe inséré dans ledit courriel;

b) L'utilisateur doit s'identifier dans ses communications professionnelles en indiquant son nom et ses coordonnées selon la façon ci-dessous (Police :Arial , 10 points, prénom et nom en gras) :

**Prénom Nom,** (titre professionnel s'il y a lieu)
Votre fonction

Votre unité administrative
Commission d'accès à l'information
Bureau 2.36
525, boulevard René-Lévesque Est
Québec (Québec) G1R 5S9
Téléphone: 418 numéro
Télécopieur: 418 numéro
adresse courriel@cai.gouv.qc.ca
www.cai.gouv.qc.ca

**Prénom Nom, (**titre professionnel s'il y a lieu)
Votre fonction

Votre unité administrative
Commission d'accès à l'information
Bureau 18.200
500, boulevard René-Lévesque Ouest
Montréal (Québec) H2Z 1W7
Téléphone: 514 numéro
Télécopieur: 514 numéro
adresse courriel@cai.gouv.qc.ca
www.cai.gouv.qc.ca

En sus de ces standards, la Commission peut au besoin demander à l'utilisateur d'ajouter d'autres éléments pour des besoins ponctuels.

## 8. CONTRÔLE DU CONTENU ET DE L'UTILISATION

La Commission se réserve le droit de demander à l'utilisateur qui atteindrait la limite de son espace de stockage, de procéder à une opération de gestion des fichiers afin qu'il respecte l'espace alloué.

La Commission se réserve également le droit, sous la supervision du responsable de la protection des renseignements personnels, d'effectuer une vérification ponctuelle du contenu et de l'utilisation des actifs informationnels et des outils informatiques de la Commission par un utilisateur, sans le consentement de ce dernier, sur autorisation de la présidente, lorsque celle-ci a des motifs sérieux de croire que l'utilisateur n'agit pas conformément aux règles de la présente directive. La présidente détermine la fréquence des vérifications et la période d'application allant jusqu'au maintien d'une surveillance constante.

Le COSI est chargé d'appliquer les mesures de contrôle, sous la supervision du responsable de la protection des renseignements personnels, et fait rapport au CSIO et au président.

## 9. SANCTIONS

L'utilisateur qui contrevient à la présente directive s'expose à des mesures disciplinaires, administratives ou légales, en fonction de la gravité de son geste. Ces mesures peuvent inclure la suspension ou le retrait des privilèges, la réprimande, la suspension, le congédiement ou toute autre mesure nécessaire, et ce, conformément aux dispositions des conventions collectives, des ententes ou des contrats.

La Commission peut transmettre à toute autorité compétente les renseignements colligés et qui lui portent à croire qu'une infraction à toute loi ou règlement en vigueur a été commise sous réserve des dispositions de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.

## 10. DISPOSITIONS FINALES

a) La présente directive entre en vigueur à la date de son approbation par la présidente;

b) La présente directive remplace la Directive sur l'utilisation des technologies de l'information de la Commission adoptée en novembre 2020;

c) Le CSIO est chargé de la mise en œuvre des dispositions de la présente directive;

d) La présente directive doit être révisée à l'occasion de changements qui pourraient l'affecter.

| | |
|---|---|
| **Diane Poitras, présidente** | **Date** |