Ministère de la Justice
Québec
Direction du Bureau du sous-ministre et du Secrétariat général

PAR COURRIEL

Le 22 février 2024

Objet : Demande d'accès aux documents – Décision
V/Réf. : sécurité de l'information
N/Réf. : BSM-2024-003548

Conformément à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, chapitre A-2.1, ci-après nommée « Loi sur l'accès »), nous avons traité votre demande d'accès reçue le 6 février 2024, laquelle se lit comme suit :

> […] Toutes mesures mise en place afin de renforcer l'encadrement de la sécurité de l'information, rehausser l'efficacité de la prise en charge des incidents et de la gestion de crise et les mécanismes de gestion mise en place afin d'améliorer la performance en cybersécurité au sein du ministère; […]
>
> (Transcription intégrale)

Décision

Nous donnons suite à votre demande. En effet, vous trouverez ci-joint le cadre normatif en matière de sécurité de l'information. Notons que ces documents sont actuellement en révision, et ce, afin de refléter nos pratiques qui sont en phase avec les dispositions légales et administratives en vigueur. D'autres documents ont été repérés, mais comme la divulgation de ceux-ci aurait pour effet de réduire l'efficacité des mesures de sécurité mises en place, ceux-ci sont protégés en vertu de l'article 29 de la Loi sur l'accès. Enfin, les brouillons ou ébauches ne sont pas visés par le droit d'accès, et ce, conformément à l'article 9 de la Loi sur l'accès. Par conséquent, ces types de documents n'ont pas été considérés lors du traitement de votre demande.

Vous trouverez ci-joint copie de l'article de loi sur lequel se fonde notre décision.

…2

Québec
Édifice Louis-Philippe-Pigeon
1200, route de l'Église, 9e étage
Québec (Québec) G1V 4M1
Téléphone : 418 643-4090
Télécopieur : 418 643-3877
www.justice.gouv.qc.ca

Recours

Conformément à l'article 51 de la Loi sur l'accès, nous vous informons que vous pouvez, en vertu de la section III du chapitre IV de cette loi (article 135 et suivants), faire une demande de révision à l'égard de cette décision en vous adressant à la Commission d'accès à l'information dans les trente (30) jours suivant la date de la présente décision. À cet effet, vous trouverez joint à la présente le document intitulé Avis de recours.

Nous vous prions d'agréer l'expression de nos sentiments les meilleurs.

Marie-Claude Daraiche, avocate
Responsable de l'accès aux documents
et de la protection des renseignements personnels

p. j. 3

Québec

À jour au 1er décembre 2023
Ce document a valeur officielle.

chapitre A-2.1

LOI SUR L'ACCÈS AUX DOCUMENTS DES ORGANISMES PUBLICS ET SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

[…]
CHAPITRE II
ACCÈS AUX DOCUMENTS DES ORGANISMES PUBLICS

SECTION I
DROIT D'ACCÈS

9. Toute personne qui en fait la demande a droit d'accès aux documents d'un organisme public.

Ce droit ne s'étend pas aux notes personnelles inscrites sur un document, ni aux esquisses, ébauches, brouillons, notes préparatoires ou autres documents de même nature.

1982, c. 30, a. 9.

[…]
SECTION II
RESTRICTIONS AU DROIT D'ACCÈS
[…]

29. Un organisme public doit refuser de confirmer l'existence ou de donner communication d'un renseignement portant sur une méthode ou une arme susceptible d'être utilisée pour commettre un crime ou une infraction à une loi.

Il doit aussi refuser de confirmer l'existence ou de donner communication d'un renseignement dont la divulgation aurait pour effet de réduire l'efficacité d'un programme, d'un plan d'action ou d'un dispositif de sécurité destiné à la protection d'un bien ou d'une personne.

1982, c. 30, a. 29; 2006, c. 22, a. 16.

[…].

AVIS DE RECOURS

RÉVISION DEVANT LA COMMISSION D'ACCÈS À L'INFORMATION

a) POUVOIR

L'article 135 de la Loi prévoit qu'une personne peut, lorsque sa demande écrite a été refusée en tout ou en partie par le responsable de l'accès aux documents ou de la protection des renseignements personnels ou dans le cas où le délai prévu pour répondre est expiré, demander à la Commission d'accès à l'information de réviser cette décision.

La demande de révision doit être faite par écrit; elle peut exposer brièvement les raisons pour lesquelles la décision devrait être révisée (art. 137).

L'adresse de la Commission d'accès à l'information est la suivante :

QUÉBEC

525, boul. René-Lévesque Est
Bureau 2.36
Québec (Québec) G1R 5S9
Tél. : 418 528-7741
Numéro sans frais : 1 888 528-7741
Télécopieur : 418 529-3102

MONTRÉAL

2045, rue Stanley
Bureau 900
Montréal (Québec) H3A 2V4
Tél. : 514 873-4196
Numéro sans frais : 1 888 528-7741
Télécopieur : 514 844-6170

b) MOTIFS

Les motifs relatifs à la révision peuvent porter sur la décision, sur le délai de traitement de la demande, sur le mode d'accès à un document ou à un enregistrement, sur les frais exigibles ou sur l'application de l'article 9 (notes personnelles inscrites sur un document, esquisses, ébauches, brouillons, notes préparatoires ou autres documents de même nature qui ne sont pas considérés comme des documents d'un organisme public).

c) DÉLAIS

Les demandes de révision doivent être adressées à la Commission d'accès à l'information dans les trente (30) jours suivant la date de la décision ou de l'expiration du délai accordé au responsable pour répondre à une demande (art. 135).

La Loi prévoit spécifiquement que la Commission d'accès à l'information peut, pour motif raisonnable, relever le requérant du défaut de respecter le délai de trente (30) jours (art. 135).

…2

APPEL DEVANT LA COUR DU QUÉBEC

a) POUVOIR

L'article 147 de la Loi sur l'accès stipule qu'une personne directement intéressée peut interjeter appel sur toute question de droit ou de compétence, devant le juge de la Cour du Québec, de la décision finale de la Commission, y compris une ordonnance de la Commission rendue au terme d'une enquête, ou, sur permission d'un juge de cette Cour, d'une décision interlocutoire à laquelle la décision finale ne pourra remédier.

b) DÉLAIS ET FRAIS

L'article 149 de la Loi sur l'accès stipule que l'appel est formé par le dépôt auprès de la Cour du Québec d'un avis à cet effet précisant les questions de droit ou de compétence qui devraient être examinées en appel.

L'avis d'appel doit être déposé au greffe de la Cour du Québec dans les trente (30) jours qui suivent la date de la réception de la décision finale par les parties.

c) PROCÉDURE

Selon l'article 151 de la Loi sur l'accès, l'avis d'appel doit être signifié aux parties et à la Commission dans les dix (10) jours de son dépôt au greffe de la Cour du Québec.

Le secrétaire de la Commission transmet au greffe, pour tenir lieu de dossier conjoint, un exemplaire de la décision contestée et les pièces de la contestation.

MINISTÈRE DE
LA **JUSTICE**
DU **QUÉBEC**

	Classification 1590 - Sécurité de l'information
	Date d'entrée en vigueur 30-10-2020
Titre **Politique ministérielle de sécurité de l'information**	Date dernière révision
Pour information **Sous-ministériat des services à l'organisation**	Date prochaine révision 30-10-2021

1. CONTEXTE

Le ministère de la Justice du Québec (ci-après le Ministère) a pour mission de favoriser la confiance des citoyens et le respect des droits individuels et collectifs par le maintien au Québec :

- d'un système de justice qui soit à la fois accessible et intègre;
- et de la primauté du droit.

Pour remplir sa mission, le Ministère recueille, produit, utilise, conserve ou détruit une importante quantité d'informations pouvant revêtir une importance stratégique pour le Ministère comme pour l'État, dont le caractère parfois hautement sensible impose des obligations additionnelles en matière de sécurité. Ces informations peuvent également avoir une valeur juridique, administrative, économique ou patrimoniale qu'il importe de préserver. En conséquence, l'information constitue une ressource essentielle qu'il convient de protéger durant tout son cycle de vie, quel qu'en soit le support ou l'emplacement.

La présente politique est adoptée en application du paragraphe (a) du premier alinéa de l'article 7 de la Directive sur la sécurité de l'information gouvernementale du Secrétariat du Conseil du trésor (SCT) (Décret 7-2014 du 15 janvier 2014). Celle-ci enjoint les organismes publics à adopter et à mettre en œuvre une politique de sécurité de l'information, à la maintenir à jour et à en assurer l'application. La mise en œuvre de cette politique est notamment soutenue par un cadre de gestion de la sécurité de l'information.

2. OBJECTIFS

La présente politique a pour objectif d'affirmer l'engagement du Ministère à s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information et d'assurer, tout au long du cycle de vie de l'information, sa disponibilité, son intégrité et sa confidentialité.

3. PORTÉE

Cette politique porte sur l'information et les actifs informationnels (ci-après actifs informationnels) dont le Ministère a la responsabilité, peu importe leur nature, leur localisation et le support sur lequel ils se trouvent, et ce, durant tout leur cycle de vie, c'est-à-dire depuis leur collecte ou leur création jusqu'à leur versement à la Bibliothèque et aux Archives nationales du Québec ou leur destruction en conformité avec le calendrier de conservation établi.

Sous réserve de politiques ou de dispositions particulières propres à certains utilisateurs, cette politique s'applique à toute personne ayant accès aux actifs informationnels du Ministère sans égard à leur statut d'emploi, y compris notamment les ressources contractuelles, les partenaires, les fournisseurs ou autres intervenants.

4. PRINCIPES DIRECTEURS

4.1. Notions générales de sécurité de l'information

4.1.1. Disponibilité

Le Ministère s'assure de la disponibilité de l'information de façon à ce qu'elle soit accessible aux entités autorisées, en temps voulu et de la manière requise.

4.1.2. Intégrité

Le Ministère s'assure de l'intégrité de l'information de manière à ce que celle-ci ne soit pas détruite ou altérée de quelque façon sans autorisation, et que le support sur lequel cette information est conservée lui procure la stabilité et la pérennité voulues.

4.1.3. Confidentialité

Le Ministère s'assure de limiter l'accès et la divulgation de l'information aux seules entités autorisées à en prendre connaissance. De plus, il recueille et conserve uniquement l'information nécessaire à l'accomplissement de sa mission, dans le respect du cadre juridique et administratif auquel il est soumis.

4.2. Le Ministère assure la sécurité de l'information conformément aux principes directeurs suivants :

4.2.1. Cadre normatif

Le Ministère s'assure que son cadre normatif et ses pratiques en matière de sécurité de l'information soient réévalués périodiquement afin de tenir compte des changements juridiques, organisationnels, technologiques, physiques et environnementaux, ainsi que de l'évolution des menaces et des risques.

4.2.2. Responsabilités et imputabilité

Le Ministère identifie clairement les responsabilités à tous les niveaux de l'organisation et met en place un processus de gestion interne de la sécurité permettant une reddition de comptes adéquate, conformément aux rôles et responsabilités définis dans le Cadre de gestion de la sécurité de l'information.

4.2.3. Sensibilisation

Le Ministère s'engage à sensibiliser et à former les utilisateurs à la sécurité de l'information, aux conséquences d'une atteinte à sa sécurité, ainsi qu'à leur rôle et à leurs obligations en cette matière.

Le Ministère s'assure que le processus de gestion de la sécurité de l'information est soutenu par une démarche d'éthique visant à assurer la régulation des conduites et la responsabilisation individuelle.

4.2.4. Gestion des actifs informationnels

Le Ministère fait l'inventaire des actifs informationnels sous sa responsabilité, peu importe leur support (ex. : papier, numérique, audio et vidéo), procède à leur catégorisation, évalue leur état de santé et détermine les mesures de protection à leur accorder.

De plus, l'information fait l'objet d'une classification de sécurité en fonction de critères touchant la valeur, les exigences juridiques, la sensibilité et la criticité de l'information pour l'organisation. Les mesures de sécurité visant à protéger l'information sont établies notamment en fonction de cette classification et tiennent compte de son contexte d'utilisation et de son cycle de vie.

4.2.5. Gestion des risques

Le Ministère procède régulièrement à des analyses de risques en vue de déterminer la protection qui doit être accordée à l'information sous sa responsabilité. Ces analyses conduisent au choix de mesures de sécurité proportionnelles aux risques, afin de les mitiger pour les amener à un niveau acceptable.

Cette analyse doit également accompagner tous les changements importants tant au niveau de l'infrastructure technologique, des processus ou de la sécurité physique.

4.2.6. Gestion des accès

Le Ministère s'engage à mettre en place un processus formel de gestion des accès pour s'assurer que les accès à l'information sont accordés selon le principe du moindre privilège, en fonction d'un profil d'accès prédéfini basé sur le rôle assumé au sein de l'organisation et sur les besoins qui en découlent pour une période requise. L'utilisation et la consultation des informations d'un système doivent se limiter aux seules personnes autorisées.

Le Ministère se réserve le droit de procéder à une habilitation sécuritaire des utilisateurs qui ont accès à ses actifs informationnels dans le cadre de leurs fonctions. Ce contrôle de sécurité doit être réalisé dans le respect des droits et libertés de la personne. De plus, le Ministère se réserve le droit d'inclure dans les contrats des clauses permettant l'habilitation sécuritaire des personnes qui auront accès à ses actifs informationnels.

4.2.7. Environnement physique

Le Ministère s'assure que les lieux physiques qu'il occupe sont adéquatement protégés, notamment contre les menaces environnementales (ex. : feu, inondation), et que des contrôles sont en place pour limiter l'accès physique aux seules personnes autorisées.

4.2.8. Acquisition, développement et maintenance des systèmes d'information

Le Ministère doit déterminer ses exigences de sécurité lors de l'acquisition de nouvelles technologies et s'assurer que ces dernières s'y conforment.

Lorsque le Ministère développe ou effectue l'entretien d'un système informatique, il doit s'assurer d'intégrer les règles et les bonnes pratiques en matière de développement sécuritaire dans sa démarche pour s'assurer de ne pas créer de vulnérabilités.

4.2.9. Contrats et ententes de service

Le Ministère s'assure de prévoir l'obligation de respecter les règles de sécurité de l'information dans les contrats et les ententes de service conclus avec des tiers tels que des prestataires de services, des partenaires ou des mandataires.

4.2.10. Gestion des incidents de sécurité de l'information

Le Ministère met en place un processus de gestion des incidents de sécurité de l'information. Il s'assure de le faire connaître à tous les utilisateurs pour qu'ils puissent identifier et signaler, sans tarder, tout acte susceptible de constituer un manquement ou un incident de sécurité.

Les incidents ou manquements doivent être documentés dans un registre formel et signalé conformément au processus établi. Ils peuvent donner lieu à une prise de mesures correctives ou de sanctions administratives.

Le Ministère déclare au réseau d'alerte gouvernemental, selon les modalités fixées par ce dernier, tout incident de sécurité de l'information à portée gouvernementale.

4.2.11. Continuité de service

Le Ministère doit prévoir les mesures nécessaires afin de s'assurer de la continuité des activités nécessaires à la réalisation de sa mission dans un délai raisonnable lors d'un sinistre ou d'un incident majeur affectant la disponibilité de l'information jugée essentielle et stratégique.

4.2.12. Sécurité opérationnelle

Le Ministère doit documenter ses procédures opérationnelles de sécurité et s'assurer qu'elles s'inscrivent dans un cadre de gestion du changement.

Le Ministère doit s'assurer que les accès aux actifs informationnels sont journalisés sur des supports sécuritaires et permettant leur exploitation. Les journaux doivent être conservés selon un calendrier établi.

Le Ministère met en place un plan de sauvegarde et de récupération des données de ses actifs informationnels afin d'assurer ses activités de reprise et de continuité des affaires.

Le Ministère met en place un processus de gestion des vulnérabilités et des mises à jour de sécurité pour ses équipements.

4.2.13. Sécurité des communications

Le Ministère s'engage à ce que son infrastructure technologique soit conçue de façon à se prémunir des menaces afin de protéger adéquatement son information.

Le Ministère s'assure de mettre en place des pratiques pour protéger les échanges d'information, au sein de cette infrastructure ou avec des tiers, afin qu'ils puissent être faits sans compromettre la confidentialité et l'intégrité de l'information.

4.2.14. Droit de regard

Le Ministère a un droit de regard sur la manipulation et l'utilisation de ses actifs informationnels par les utilisateurs à partir des équipements normalisés du Ministère. Ce droit s'exerce en conformité avec le cadre juridique et administratif applicable au Ministère sous réserve de dispositions particulières propres à certains utilisateurs.

5. CADRE NORMATIF

La présente politique doit être interprétée et appliquée conformément aux lois, aux règlements et aux autres textes normatifs énumérés à l'annexe I.

6. MODALITÉS D'APPLICATION

Les modalités d'application de la présente politique se retrouvent dans les documents formant le cadre normatif de la sécurité de l'information, notamment dans des politiques, des cadres de gestion, des directives, des guides et des procédures.

7. RÔLES ET RESPONSABILITÉS DES INTERVENANTS

Les rôles et responsabilités des intervenants ci-dessous sont détaillés dans le Cadre de gestion de la sécurité de l'information.

7.1. La sous-ministre

La sous-ministre est la première responsable de la sécurité de l'information relevant de son autorité. Elle doit assurer le respect des lois et des règles de sécurité de l'information déterminées par le SCT, notamment en ce qui a trait à la mise en place de mesures permettant la réduction des risques reliés à la sécurité de l'information.

7.2. Dirigeant de l'information

Le dirigeant de l'information (DI) est responsable de veiller à l'application, par chaque organisme public auquel il est rattaché, des règles de gouvernance et de gestion établies en vertu de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement.

7.3. Le responsable organisationnel de la sécurité de l'information

La sous-ministre désigne le responsable organisationnel de la sécurité de l'information (ROSI). Le ROSI joue le rôle de porte-parole du dirigeant principal de l'information (DPI) et relaie au Ministère les orientations et les priorités d'intervention gouvernementale en sécurité de l'information. Il assure la coordination et la cohérence des mesures de sécurité de l'information mises en œuvre par d'autres intervenants du Ministère. Il coordonne également la contribution du Ministère aux processus de gestion des risques et de gestion des incidents à portée gouvernementale.

7.4. Le responsable de la sécurité des actifs informationnels

Le responsable de la sécurité des actifs informationnels (RSAI) appuie et conseille le ROSI dans son rôle de coordination afin d'assurer la cohérence des mesures de sécurité mises en œuvre au Ministère.

7.5. Le conseiller organisationnel en sécurité de l'information

Le COSI apporte le soutien nécessaire aux différents intervenants, notamment en ce qui a trait à la mise en œuvre des mesures d'atténuation des risques et à la mise en place de processus formels de sécurité de l'information.

Le COSI est de plus responsable de la révision de la présente politique afin de s'assurer de son adéquation aux besoins du Ministère.

7.6. Le coordonnateur organisationnel de gestion des incidents

Le COGI est désigné par la sous-ministre et apporte le soutien technique nécessaire aux différents intervenants. Il participe activement au réseau d'alertes gouvernemental et contribue à la mise en place du processus de gestion des incidents de sécurité de l'information au sein du Ministère et du processus de gestion des incidents à portée gouvernementale.

7.7. Le détenteur de l'information

Le détenteur de l'information est une personne désignée par la sous-ministre pour assumer la responsabilité de la catégorisation des actifs informationnels et de la classification de l'information, de l'identification et de la mise en œuvre des mesures de sécurité propres à assurer la protection de l'information collectée, utilisée, communiquée, conservée ou détruite.

Chaque détenteur de l'information collabore étroitement avec les différents intervenants, notamment à la détermination des exigences de sécurité, à la gestion des incidents et à la reddition de comptes en matière de sécurité.

7.8. Le gestionnaire

Le gestionnaire doit faire connaître au personnel de son unité les règles de sécurité de l'information et veiller à leur application. Il autorise les demandes d'accès aux actifs informationnels nécessaires à l'exercice de leurs fonctions et les révoque en conformité avec les règles applicables.

7.9. L'utilisateur

Tout utilisateur a l'obligation de protéger l'information mise à sa disposition par le Ministère. À cette fin, il doit notamment :

a) prendre connaissance de la présente politique, des directives, des guides et autres lignes de conduite en découlant, y adhérer et prendre l'engagement de s'y conformer;

b) signaler immédiatement à la personne désignée ou à son gestionnaire, conformément au processus établi en matière de gestion des incidents de sécurité, tout acte ou toute situation pouvant nuire à la protection de l'information;

c) utiliser, à l'intérieur des droits d'accès qui lui sont attribués et uniquement lorsqu'elle est nécessaire à l'exercice de ses fonctions, l'information mise à sa disposition en se limitant aux fins auxquelles elle est destinée;

d) respecter les mesures de sécurité mises en place sur son poste de travail et sur tout équipement contenant de l'information à protéger, et ne doit pas modifier leur configuration ni les désactiver;

e) remettre les différentes cartes d'identité et d'accès, ainsi que tout document appartenant au Ministère, à la fin de l'exercice de ses fonctions.

8. DISPOSITIONS FINALES

Sanctions et mesures disciplinaires

Toute personne qui contrevient à la présente politique ou directive en découlant s'expose à des sanctions dont des mesures disciplinaires, administratives ou à des recours judiciaires.

Lorsqu'une vérification ou une enquête permet de soupçonner qu'une infraction à une loi ou à un règlement a été commise, la sous-ministre peut également informer toute autre autorité compétente pour vérifier notamment s'il y a matière à poursuite.

Mesures d'exception

Le détenteur de l'information qui a une raison valable de ne pas se conformer à une exigence particulière ou de ne pas recourir à une mesure de sécurité déterminée peut demander une mesure d'exception au ROSI après avoir pris soin d'évaluer les risques associés à la mesure d'exception. Ces exceptions doivent être documentées et rendues disponibles au ROSI et au RSAI.

Mise en œuvre, suivi et révision

Le ROSI est chargé de la mise en œuvre des dispositions de la présente politique et de ses directives d'application.

La présente politique est complétée par le Cadre de gestion de la sécurité de l'information et les obligations qui en découlent sont précisées par des directives.

La présente politique doit être revue annuellement suivant son adoption ou à la suite d'un changement qui justifie une révision.

9. ANNEXE

ANNEXE 1
Cadre juridique et administratif

CANADA

- Charte canadienne des droits et libertés de la Loi constitutionnelle de 1982
- Code criminel, L.R., 1985, c. C-46

QUÉBEC

Lois et règlements

- Code civil du Québec, RLRQ, c. CCQ-1991
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ, c. A-2.1 :
  - Règlement sur la diffusion de l'information et sur la protection des renseignements personnels, RLRQ, c. A-2.1, r. 2
- Loi sur les archives, RLRQ, c. A-21.1
- Loi concernant le cadre juridique des technologies de l'information, RLRQ, c. C-1.1
- Charte des droits et libertés de la personne, RLRQ, c. C-12
- Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, RLRQ, c. G-1.03
- Loi sur le ministère de la Justice, RLRQ, c. M-19
- Loi sur les tribunaux judiciaires, RLRQ, c. T-16

MINISTÈRE DE
LA **JUSTICE**
DU **QUÉBEC**

	Classification 1590 - Sécurité de l'information
	Date d'entrée en vigueur 30-10-2020
Titre **Politique ministérielle de sécurité de l'information**	Date dernière révision
Pour information **Sous-ministériat des services à l'organisation**	Date prochaine révision 30-10-2021

Politiques, cadres et directives

- Politique ministérielle d'utilisation du courriel, des services d'Internet et du collecticiel
- Directive sur la sécurité de l'information gouvernementale, décret 7-2014 du 15 janvier 2014
- Cadre gouvernemental de gestion - Sécurité de l'information (2014)

Date :

La sous-ministre de la Justice
et sous-procureure générale,

Line Drouin

HISTORIQUE

Description du changement	Approbation	Date
Adoption de la politique ministérielle concernant la sécurité de l'information	Sous-ministre	30-10-2020

MINISTÈRE DE
LA **JUSTICE**
DU **QUÉBEC**

	Classification 1590 - Sécurité de l'information
	Date d'entrée en vigueur 30-10-2020
Titre **Cadre de gestion de la sécurité de l'information**	Date dernière révision
Pour information **Sous-ministériat des services à l'organisation**	Date prochaine révision 30-10-2025

DISPOSITIONS

1. INTRODUCTION

Le présent cadre est adopté en application de la Politique ministérielle de sécurité de l'information. Il vise à renforcer la gouvernance de la sécurité de l'information du Ministère par la mise en place d'une structure organisationnelle de la sécurité de l'information ainsi que la définition des rôles et responsabilités à tous les niveaux du Ministère.

2. CADRE NORMATIF

Le présent cadre de gestion doit être interprété et appliqué conformément au cadre juridique et administratif en annexe de la Politique ministérielle de sécurité de l'information.

3. RÔLES ET RESPONSABILITÉS DES INTERVENANTS

3.1. La sous-ministre

La sous-ministre est la première responsable de la sécurité de l'information relevant de son autorité. Elle doit assurer le respect des lois et des règles de sécurité de l'information déterminées par le Secrétariat du Conseil du trésor (SCT), notamment en ce qui a trait à la mise en place de mesures permettant la réduction des risques reliés à la sécurité de l'information. À ce titre, elle doit notamment :

a) adopter les orientations stratégiques de la sécurité de l'information du Ministère, la politique, le cadre de gestion, les directives et les plans d'action en la matière et en assurer la mise en oeuvre;

b) approuver les bilans de sécurité de l'information avant transmission au SCT;

c) s'assurer de la mise en place de mesures permettant de réduire les risques de sécurité de l'information à un niveau acceptable par le Ministère;

d) s'assurer de l'adéquation des mesures de sécurité de l'information en vigueur par rapport aux risques encourus;

e) s'assurer de la mise en oeuvre 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;

f) s'assurer de la réalisation périodique d'audits de sécurité de l'information et de tests d'intrusion et de vulnérabilité, conformément aux énoncés de la Directive sur la sécurité de l'information gouvernementale (décret 7-2014 du 15 janvier 2014), et en dégager les priorités d'action ainsi que les échéanciers afférents;

g) favoriser l'utilisation des services communs de sécurité de l'information déterminés par le SCT;

h) s'assurer 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;

i) s'assurer 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;

j) approuver et présenter 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;

k) désigner les détenteurs de l'information, le responsable organisationnel de la sécurité de l'information (ROSI) et le coordonnateur organisationnel de gestion des incidents (COGI);

l) s'assurer de la saine gouvernance de la sécurité de l'information et veiller à en établir les objectifs stratégiques;

m) déléguer sa responsabilité au ROSI de déclarer les incidents de sécurité de l'information à portée gouvernementale à l'équipe de réponse aux incidents de sécurité de l'information de l'Administration québécoise (CERT/AQ).

3.2. Dirigeant de l'information

Le dirigeant de l'information (DI) est responsable de veiller à l'application, par chaque organisme public auquel il est rattaché, des règles de gouvernance et de gestion établies en vertu de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement. À ce titre, il doit notamment :

a) définir des règles particulières en matière de gestion de l'information, incluant celles inhérentes à la sécurité de l'information, qui seront applicables aux organismes publics auxquels il est rattaché;

b) veiller à la pérennité des actifs informationnels des organismes publics auxquels il est rattaché.

3.3. Le responsable organisationnel de la sécurité de l'information

La sous-ministre désigne le ROSI. Le ROSI joue le rôle de porte-parole du dirigeant principal de l'information (DPI) et relaie au Ministère les orientations et les priorités d'intervention gouvernementales en sécurité de l'information. Il assure la coordination et la cohérence des mesures de sécurité de l'information mises en œuvre par d'autres intervenants du Ministère. Il coordonne également la contribution du Ministère aux processus de gestion des risques et de gestion des incidents à portée gouvernementale. À ce titre, il doit notamment :

a) soumettre, aux fins de recommandation pour approbation de la sous-ministre ou de consultation au Comité ministériel de la sécurité de l'information (CMSI), les orientations, les politiques, les directives, les cadres de gestion, les priorités d'action, les éléments de reddition de comptes ainsi que tout événement ayant mis ou aurait pu mettre en péril la sécurité de l'information;

b) s'assurer de la coordination et de la cohérence des actions de sécurité de l'information menées au sein du Ministère par d'autres intervenants, dont notamment les détenteurs de l'information ainsi que les unités responsables des ressources informationnelles, de l'accès à l'information et de la protection des renseignements personnels, de la gestion documentaire, de la sécurité physique et de l'éthique;

c) déclarer au dirigeant principal de l'information les risques de sécurité de l'information à portée gouvernementale;

d) déclarer au CERT/AQ les incidents de sécurité de l'information à portée gouvernementale;

e) recommander à la sous-ministre, pour approbation, 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;

f) coordonner l'élaboration et la mise en oeuvre d'un programme continu de formation et de sensibilisation en matière de sécurité de l'information;

g) participer aux tables de coordination et de concertation gouvernementales en matière de sécurité de l'information;

h) participer à des comités interministériels et représenter le Ministère en matière de sécurité de l'information;

i) autoriser une mesure d'exception au détenteur de l'information qui a une raison valable de ne pas se conformer à une exigence particulière ou de ne pas recourir à une mesure de sécurité déterminée;

j) déterminer la composition du CMSI et du comité ministériel de gestion de crise.

3.4. Le responsable de la sécurité des actifs informationnels

Le responsable de la sécurité des actifs informationnels (RSAI) appuie et conseille le ROSI dans son rôle de coordination afin d'assurer la cohérence des mesures de sécurité mises en œuvre au Ministère. À ce titre, il doit notamment :

a) proposer au ROSI les orientations, les politiques, les directives, les cadres de gestion, les priorités d'action, les éléments de reddition de comptes et les mettre en oeuvre;

b) élaborer et mettre en oeuvre un programme de formation continue et de sensibilisation en matière de sécurité de l'information;

c) produire les bilans de sécurité de l'information et identifier les risques à portée gouvernementale;

d) mettre en œuvre les orientations et les priorités d'intervention gouvernementales en matière de sécurité de l'information;

e) s'assurer de l'intégration de la sécurité dans les projets et les initiatives afin que les risques demeurent à un niveau acceptable pour le Ministère;

f) réaliser périodiquement des audits de sécurité de l'information et des tests d'intrusion et de vulnérabilité, conformément aux énoncés de la Directive sur la sécurité de l'information gouvernementale, et en dégager les priorités d'action ainsi que les échéanciers afférents;

g) mettre en oeuvre les processus officiels de sécurité de l'information permettant notamment la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents et en coordonner l'application;

h) gérer la réponse aux incidents de sécurité de l'information et faire rapport au ROSI de tout incident de sécurité de l'information;

i) mettre à jour le présent cadre de gestion.

3.5. Le conseiller organisationnel en sécurité de l'information

Le COSI apporte son soutien aux différents intervenants, notamment en ce qui a trait à la mise en œuvre des mesures d'atténuation des risques et à la mise en place de processus formels de sécurité de l'information.

Le COSI est de plus responsable de la révision annuelle de la Politique ministérielle de sécurité de l'information afin de s'assurer de son adéquation aux besoins du Ministère. À ce titre, il doit notamment :

a) contribuer à la mise en œuvre des orientations internes découlant des directives gouvernementales, des politiques internes et des pratiques généralement admises à cet égard;

b) conseiller le Ministère en matière d'ententes de service et de contrats et formuler des recommandations quant à l'intégration de dispositions garantissant le respect des exigences de sécurité de l'information;

c) tenir à jour le registre d'autorité de la sécurité de l'information;

d) tenir à jour le registre de catégorisation et transmettre au CMSI l'analyse de la catégorisation pour recommandation;

e) assister les détenteurs de l'information dans l'exercice de catégorisation concernant les systèmes qui traitent de l'information relevant de leur responsabilité et dans la réalisation des analyses de risques de sécurité des actifs informationnels;

f) contribuer à la définition et à la mise en œuvre des processus formels de sécurité de l'information.

3.6. Le coordonnateur organisationnel de gestion des incidents

Le COGI est désigné par la sous-ministre et collabore étroitement avec les différents intervenants afin de leur fournir le soutien technique nécessaire à l'exercice de leurs responsabilités. Il participe activement au réseau d'alertes gouvernemental et contribue à la mise en place du processus de gestion des incidents de sécurité de l'information au sein du Ministère et du processus de gestion des incidents à portée gouvernementale. À ce titre, il doit notamment :

a) contribuer aux analyses de risques de sécurité de l'information, identifier les menaces et les situations de vulnérabilité et mettre en œuvre les solutions appropriées;

b) contribuer à la définition, la mise en œuvre et l'exécution des processus formels de sécurité de l'information, dont notamment celui concernant les incidents de sécurité de l'information tant à portée ministérielle que gouvernementale;

c) collaborer à l'élaboration et à la mise à jour des guides portant sur la sécurité opérationnelle notamment des systèmes, des réseaux et des infrastructures;

d) collaborer étroitement avec les différents intervenants et leur fournir le soutien technique nécessaire à l'exercice de leurs responsabilités;

e) coordonner la réponse aux incidents de sécurité de l'information.

3.7. Le détenteur d'information

Le détenteur de l'information est la personne désignée par la sous-ministre pour assumer la responsabilité de la catégorisation des actifs informationnels et de la classification de l'information, de l'identification et de la mise en œuvre des mesures de sécurité propres à assurer la protection de l'information collectée, utilisée, communiquée, conservée ou détruite.

Chaque détenteur de l'information collabore étroitement avec les différents intervenants, notamment à la détermination des exigences de sécurité, à la gestion des incidents et à la reddition de comptes en matière de sécurité. À ce titre, il doit notamment :

a) identifier les besoins en matière de sécurité et s'assurer que des mesures de sécurité appropriées sont élaborées, mises en place et appliquées systématiquement;

b) approuver le choix des mesures appropriées pour la protection de l'information dont il est responsable ainsi que des moyens de contrôle et des règles d'accès à cette information;

c) déléguer au besoin, à des représentants qu'il désigne, certaines responsabilités en matière de sécurité de l'information;

d) catégoriser l'information relevant de sa responsabilité selon sa valeur et ses exigences en matière de disponibilité, d'intégrité et de confidentialité;

e) classifier l'information relevant de sa responsabilité selon sa valeur et sa sensibilité;

f) veiller à ce que les mesures de sécurité de l'information, y compris celles reliées au respect des exigences légales de protection des renseignements personnels, soient mises en place et appliquées;

g) agir comme maître d'œuvre de la gestion des risques de ses actifs informationnels en sélectionnant et approuvant les mesures de sécurité de l'information adéquates et proportionnelles aux risques, tout en assumant les risques résiduels;

h) s'assurer du respect des lois, des politiques, des normes, des cadres de gestion et des processus en matière de sécurité de l'information dans les procédures opérationnelles, techniques ou administratives, relativement à l'information relevant de sa responsabilité;

i) autoriser les accès aux actifs informationnels sous sa responsabilité;

j) maintenir à jour les procédures et les listes des privilèges d'accès des personnes autorisées.

3.8. Le gestionnaire

Le gestionnaire doit faire connaître au personnel de son unité les règles de sécurité de l'information et veiller à leur application. Il autorise les demandes d'accès aux actifs informationnels nécessaires à l'exercice de leurs fonctions et les révoque en conformité avec les règles applicables. Il doit notamment :

a) s'assurer que le personnel de son unité est informé et sensibilisé à la sécurité de l'information et sur les modalités de sa mise en œuvre;

b) indiquer clairement au personnel de son unité le rôle et les obligations de l'utilisateur ainsi que les conséquences d'une atteinte à la sécurité de l'information;

c) s'assurer que l'information est utilisée en conformité avec les politiques, les directives, les processus et les consignes en matière de sécurité de l'information;

d) autoriser au personnel de son unité l'accès aux seuls actifs informationnels nécessaires à l'exercice de leurs fonctions;

e) aviser l'assistance technique de tout problème ou risque pouvant affecter la disponibilité, l'intégrité ou la confidentialité de l'information.

3.9. Le responsable de l'audit interne

Il joue un rôle-clé dans la reddition de comptes en matière de sécurité de l'information, plus particulièrement en regard de l'identification, de l'évaluation et de la gestion des risques d'atteinte à la sécurité de l'information. À ce titre, il doit évaluer, examiner ou vérifier :

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.

Il peut réaliser, sur demande, des enquêtes administratives concernant des cas possibles de dérogation, de non-respect ou d'atteinte aux règles relatives à la sécurité de l'information au MJQ.

Les comités sur la sécurité de l'information

3.10. Le Comité ministériel de la sécurité de l'information

Le CMSI est la principale instance de concertation en matière de sécurité et les membres sont nommés par le ROSI. En vue de l'approbation par la sous-ministre, son mandat consiste à assurer la cohérence des actions avec les orientations, politiques, directives et autres dispositions gouvernementales, à examiner et formuler des recommandations concernant :

a) les orientations, politiques, directives, cadres de gestion, plans d'action et bilans de l'organisation en matière de sécurité de l'information;

b) les propositions de mesures, les projets et autres éléments stratégiques en matière de sécurité de l'information;

c) les analyses de risques et les mesures à mettre en place pour protéger les actifs informationnels de l'organisation.

3.11. L'équipe de réponse aux incidents de sécurité de l'information

L'équipe de réponse aux incidents de sécurité de l'information est un groupe ad hoc présidé par le COGI et composé de personnes jugées pertinentes à la prise en charge d'un incident de sécurité. Elle a notamment pour rôle de :

a) procéder à la résolution de l'incident de sécurité de l'information;

b) convoquer toute personne jugée utile à la compréhension et la résolution de l'incident de sécurité de l'information.

3.12. Le Comité ministériel de gestion de crise

Le Comité ministériel de gestion de crise est le groupe décisionnel appelé à intervenir en cas d'incident critique de sécurité de l'information, 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 notamment pour rôle :

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 poser en cas de sinistre;

e) de formuler des recommandations concernant le délestage, en totalité ou en partie, des activités de l'organisation;

f) de communiquer avec les médias.

La composition du Comité ministériel de gestion de crise est déterminée par le ROSI.

4. DISPOSITIONS FINALES

4.1. Mise en œuvre, suivi et révision

Le ROSI, appuyé par le RSAI, est responsable de l'élaboration et de l'application du cadre de gestion.

Ce cadre sera révisé à l'occasion de changements importants qui pourraient l'affecter ou, au plus tard, tous les cinq ans à partir de la date d'approbation. Toute modification devra être approuvée par la sous-ministre sur recommandation du CMSI.

	Classification 1590 - Sécurité de l'information
	Date d'entrée en vigueur 30-10-2020
Titre **Cadre de gestion de la sécurité de l'information**	Date dernière révision
Pour information **Sous-ministériat des services à l'organisation**	Date prochaine révision 30-10-2025

5. ENTRÉE EN VIGUEUR ET APPROBATION

Le présent cadre entre en vigueur à la date de sa signature par la sous-ministre.

Date :

La sous-ministre de la Justice
et sous-procureure générale,

Line Drouin

SOUS-MINISTÉRIAT
ADJOINT DES SERVICES
À L'ORGANISATION

Offre de services

Direction de la sécurité des systèmes d'information

OFFRIR UNE JUSTICE CENTRÉE SUR LES besoins des CITOYENNES ET DES CITOYENS

Justice Québec

SOUS-MINISTÉRIAT
ADJOINT DES SERVICES
À L'**ORGANISATION**

Équipe de la cyberdéfense

Les services offerts par l'équipe de la cyberdéfense (COCD) consistent à :

- ✓ Contrôler les risques reliés à la SI en exerçant une surveillance des infrastructures, une veille des menaces et un suivi des vulnérabilités;
- ✓ Coordonner la résolution des incidents de sécurité et faire le lien avec le Centre gouvernemental de cyberdéfense (CGCD);
- ✓ Collaborer aux initiatives gouvernementales de cyberdéfense;
- ✓ Produire les tableaux de bord en sécurité de l'information;
- ✓ Certifier les accès aux systèmes, applications et infrastructures ministériels;
- ✓ S'assurer de la conformité des activités en matière de gestion des identités et des accès.

OFFRIR UNE JUSTICE CENTRÉE SUR LES besoins des CITOYENNES ET DES CITOYENS

Centre opérationnel de cyberdéfense
COCD@justice.gouv.qc.ca

SOUS-MINISTÉRIAT
ADJOINT DES SERVICES
À L'**ORGANISATION**

Centre opérationnel en cyberdéfense (COCD)

Le COCD est une unité administrative du MJQ spécialisée en sécurité de l'information offrant des services au ministère et aux organismes publics relevant du portefeuille du ministre ainsi qu'à la Magistrature.

Les services offerts en lien avec la gestion des menaces, des vulnérabilités et des incidents (GMVI) consistent à :

- ✓ Balayage des vulnérabilités des sites exposés sur Internet réalisé par le COCD du MJQ à partir de la solution infonuagique gouvernementale;
- ✓ Balayage des vulnérabilités sur les sites non exposés , réalisés par le COCD du MJQ;
- ✓ Coordination des résolutions des vulnérabilités signalées par le public au CGCD sur la plate-forme PSV;
- ✓ Soutien aux organismes en cas d'incidents affectant la sécurité;
- ✓ Des tests d'intrusions sur les sites exposés et non exposés;
- ✓ Assurer la surveillance des services en temps réel;
- ✓ Exploitation des journaux en cas d'incidents;
- ✓ Communication, suivi des plans d'action et reddition de compte.

En plus des opérations précitées, le ROCD et son COCD doivent :

- ✓ Développer une vision stratégique de la cyberdéfense en s'assurant de la mutualisation des ressources mises à leur disposition;
- ✓ S'assurer de développer les processus requis et les différents cahiers de réponses « playbooks » permettant de répondre à tous types d'évènements affectant la sécurité du ministère et de ses clients;
- ✓ S'assurer de la mise en œuvre et l'opérationnalisation des processus élaborés;
- ✓ Élaborer un plan de gestion de crise et prise en charge des évènements affectant la sécurité;
- ✓ Conduire des audits techniques de conformité aux bonnes pratiques et rectifier les écarts moyennant les communications appropriées.

OFFRIR UNE JUSTICE CENTRÉE SUR LES besoins des CITOYENNES ET DES CITOYENS

SOUS-MINISTÉRIAT ADJOINT DES SERVICES À L'ORGANISATION

Équipe de l'architecture de sécurité

Les services offerts par l'équipe de l'architecture de sécurité consistent à :

- ✓ Établir les exigences et produire des avis en matière de sécurité de l'information (SI);
- ✓ S'assurer de l'adéquation entre les mesures de protection et la sensibilité des actifs informationnels;
- ✓ Piloter la feuille de route de la SI;
- ✓ Analyser les risques reliés à la SI et proposer des mesures de mitigation;
- ✓ Accompagner les projets dans l'élaboration de solutions répondant aux exigences en matière de SI;
- ✓ S'assurer de la conformité des solutions en regard des exigences établies en matière de SI.

OFFRIR UNE JUSTICE CENTRÉE SUR LES besoins des CITOYENNES ET DES CITOYENS

SOUS-MINISTÉRIAT ADJOINT DES SERVICES À L'ORGANISATION

Équipe de la reprise informatique

Les services offerts par l'équipe de la reprise informatique consistent à :

- ✓ Proposer et implanter la stratégie de relève informatique en cas de sinistre majeur ou cyberattaque;
- ✓ Réaliser le plan de reprise informatique au Ministère selon la stratégie établie;
- ✓ Coordonner l'activation de la reprise en cas de sinistre majeur ou cyberattaque;
- ✓ Coordonner les exercices annuels de relève informatique;
- ✓ Veiller à la sécurisation des copies de sauvegardes des actifs informationnels;
- ✓ S'assurer que l'ensemble des intervenants connaissent leurs rôles et responsabilités en cas de sinistre;
- ✓ Rédiger un plan de formation sur le plan de reprise;
- ✓ Former les intervenants;
- ✓ Rédiger le plan de gestion de crise du comité de crise opérationnel (CCO);
- ✓ Participation au CCO en cas de crise;
- ✓ Rédaction et actualisation des procédures selon les changements aux infrastructures du ministère.

OFFRIR UNE JUSTICE CENTRÉE SUR LES besoins des CITOYENNES ET DES CITOYENS

SOUS-MINISTÉRIAT ADJOINT DES SERVICES À L'ORGANISATION

Équipe de la gouvernance de la sécurité de l'information

Les services offerts par l'équipe Formation et sensibilisation à la sécurité de l'information consistent à :

- ✓ Élaborer et mettre en œuvre un plan de formation et sensibilisation pour l'ensemble des utilisateurs des infrastructures et applications du Ministère;
- ✓ Concevoir le matériel de formation et sensibilisation en collaboration avec les conseillers en sécurité et les partenaires;
- ✓ Diffuser le matériel de formation et sensibilisation.

OFFRIR UNE JUSTICE CENTRÉE SUR LES besoins des CITOYENNES ET DES CITOYENS

SOUS-MINISTÉRIAT ADJOINT DES SERVICES À L'ORGANISATION

Équipe de la gouvernance de la sécurité de l'information

Les services offerts par l'équipe de la gouvernance de la sécurité de l'information consistent à :

- ✓ Élaborer et suivre la mise en œuvre du cadre normatif de la sécurité de l'information incluant:
  - ➢ La stratégie et le programme triennal ministériel de sécurité de l'information
  - ➢ La politique ministérielle de sécurité de l'information
  - ➢ Le cadre de gestion de la sécurité de l'information
  - ➢ Les Directives de Sécurité de l'information
- ✓ Élaborer et mettre en œuvre le processus de gestion des risques de sécurité de l'information;
- ✓ Maintenir les registres d'autorité et de catégorisation des actifs informationnels;
- ✓ S'assurer de la reddition des comptes et gérer la performance (tableaux de bord).

OFFRIR UNE JUSTICE CENTRÉE SUR LES besoins des CITOYENNES ET DES CITOYENS

SOUS-MINISTÉRIAT ADJOINT DES SERVICES À L'ORGANISATION

Équipe de l'encadrement et de l'architecture de la gestion des identités et des accès (GIA)

Les services offerts par l'équipe de l'encadrement et de l'architecture GIA consistent à :

- ✓ Modéliser les rôles à l'échelle de l'organisation pour en faciliter la gestion
- ✓ Piloter la solution du courtier d'identité au ministère
- ✓ Contrôler, surveiller et rendre compte de la gestion des identités et des accès aux autorités
- ✓ Auditer ou coordonner les audits en lien avec la GIA
- ✓ Réviser les processus GIA et les diffuser auprès des parties prenantes
- ✓ Gérer les autorisations liées à une identité selon un modèle par rôle (RBAC).

OFFRIR UNE JUSTICE CENTRÉE SUR LES besoins des CITOYENNES ET DES CITOYENS