Ministère
de la Famille
Québec

Direction générale du Bureau de la sous-ministre et du Secrétariat général

PAR COURRIEL

[redacted],

La présente donne suite à votre demande d'accès à l'information reçue 12 décembre 2025, par laquelle vous souhaitez obtenir une copie des documents ou renseignements suivants :

> « *1- Une copie des politiques, directives ou lignes directrices encadrant les obligations du ministère de la Famille afin que la protection des données personnelles des utilisateurs (prestataires, parents ou enfants) du Portail d'inscription aux services éducatifs soit assurée.*
>
> *2- Tout document décrivant les mesures prises par le ministère de la Famille pour s'assurer que Force.com met en place les moyens nécessaires afin de garantir la confidentialité des données personnelles des utilisateurs (prestataires, parents ou enfants) du Portail d'inscription aux services éducatifs. »*

Conformément à l'article 47 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1) (ci-après désignée « la Loi sur l'accès »), nous vous informons du résultat des recherches menées lors du traitement de votre demande.

En réponse au premier volet, nous vous transmettons la documentation visée par votre requête. À sa lecture, vous constaterez que nous avons soustrait des renseignements personnels de nature confidentielle.

En réponse au deuxième volet, nous comprenons de votre requête que vous faites référence à l'acquisition par le ministère de la Famille d'outils de sécurité auprès du fournisseur Salesforce.

Le contrat conclu avec le fournisseur de services Salesforce comporte des clauses spécifiques relatives à la protection des renseignements personnels, auxquelles ce dernier est tenu de se conformer. Par ailleurs, des tests d'intrusion et l'inscription au programme de prime aux bogues ont été réalisés pour le Portail d'inscription aux services de garde (Portail), afin de garantir un niveau de protection adéquat, et ce, en collaboration avec le ministère de la Cybersécurité et du Numérique. Enfin, l'utilisation du service d'authentification gouvernementale pour accéder au Portail constitue une mesure supplémentaire visant à assurer la sécurité et la protection des données.

…2

425, rue Jacques-Parizeau, 4e étage
Québec (Québec) G1R 4Z1
Téléphone : 418 528-7100, poste 82725
Télécopieur : 418 646-0985
www mfa gouv qc.ca

Vous trouverez en pièce jointe un extrait du contrat intervenu avec la firme Salesforce relativement à ces éléments. À sa lecture, vous remarquerez que les informations quant à l'identité numérique de celle-ci ont été soustraites, puisqu'elles permettent d'accéder au contrat dans son intégralité. De plus, nous avons caviardé en gris des passages lorsqu'ils ne sont pas visés par votre demande.

Finalement, d'autres documents en notre possession ne peuvent vous être transmis puisqu'ils contiennent des renseignements ayant des incidences sur des mesures de sécurité quant à la protection de nos infrastructures technologiques.

Nous invoquons à l'appui de notre décision les articles 14, 29, 53, 54 et 56 de la Loi sur l'accès.

Si vous désirez contester cette décision, il vous est possible de le faire auprès de la Commission d'accès à l'information. Vous trouverez, ci-annexée, une note explicative concernant l'exercice de ce recours.

Veuillez agréer, [redacted], mes sincères salutations.

Cynthia Richard
Responsable ministérielle de l'accès aux documents
et de la protection des renseignements personnels

p. j. 2

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

14. Un organisme public ne peut refuser l'accès à un document pour le seul motif que ce document comporte certains renseignements qu'il doit ou peut refuser de communiquer en vertu de la présente loi.

Si une demande porte sur un document comportant de tels renseignements, l'organisme public peut en refuser l'accès si ces renseignements en forment la substance. Dans les autres cas, l'organisme public doit donner accès au document demandé après en avoir extrait uniquement les renseignements auxquels l'accès n'est pas autorisé.

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.

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

1° la personne concernée par ces renseignements consent à leur divulgation;

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.

56. Le nom d'une personne physique n'est pas un renseignement personnel, sauf lorsqu'il est mentionné avec un autre renseignement la concernant ou lorsque sa seule mention révélerait un renseignement personnel concernant cette personne.

Avis de recours

À la suite d'une décision rendue en vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*.

Révision par la Commission d'accès à l'information

a) Pouvoir **:**

L'article 135 de la Loi prévoit qu'une personne dont la 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 peut 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-Levesque Est Bureau 2.36 Québec (Québec) G1R 5S9	Tél. : 418 528-7741 Numéro sans frais 1 888 -528-7741	Téléc. : 418 529-3102
Montréal	500, boul. René Lévesque Ouest Bureau 18.200 Montréal (Québec) H2Z 1W7	Tél. : 514 873-4196 Numéro sans frais 1 888 -528-7741	Téléc. : 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 renseignement, 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 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 30 jours (art. 135).

Volet # 1

Politique sur la gestion et la protection des renseignements personnels

SEPTEMBRE 2023

Votre gouvernement

Québec

Coordination et rédaction
Direction du bureau de la sous-ministre
Comité sur l'accès à l'information et la protection
des renseignements personnels

Pour information :
Centre des relations avec la clientèle
Ministère de la Famille
600, rue Fullum, 5e étage
Montréal (Québec) H2K 4S7
Ligne sans frais : 1 855 336-8568

Table des matières

Préambule

La *Loi sur l'accès aux documents des organismes publics et la protection des renseignements personnels* (RLRQ, chapitre A-2. 1) (*Loi sur l'accès*) et les règlements adoptés en vertu de celle-ci ont pour objet d'encadrer l'accès aux documents et la protection des renseignements personnels détenus par les organismes publics.

Dans le cadre de ses activités, le ministère de la Famille (Ministère) traite des renseignements personnels qui concernent les membres de son personnel et des personnes utilisant ses services ou agissant à titre de partenaires d'affaires. À l'exception de celles qui ont un caractère public aux termes de cette loi, ces données sont confidentielles.

Le Ministère a ainsi la responsabilité d'assurer la confidentialité de ces renseignements personnels et d'en garantir une utilisation conforme aux obligations qui lui incombent à leur égard, notamment d'obtenir le consentement valide des personnes concernées avant de les communiquer à de tierces parties. La Politique sur la gestion et la protection des renseignements personnels (Politique) met en place des mesures concrètes à ces fins.

1. Objectifs

La présente politique vise à soutenir le Ministère et son personnel dans l'exercice des responsabilités et dans l'exécution des obligations prévues par la *Loi sur l'accès*. Elle encadre la protection et l'utilisation des renseignements personnels tout au long de leur cycle de vie et définit les rôles et responsabilités de chaque intervenant, interne ou externe, en fonction de leurs activités au sein de l'organisation.

2. Champ d'application

La présente politique s'applique à tous les membres du personnel ainsi qu'à toute personne qui, dans le cadre de ses fonctions, a accès à des renseignements personnels détenus par le Ministère lorsqu'ils recueillent, utilisent, communiquent, conservent ou détruisent des renseignements personnels, quel que soit leur support, et ce, de leur collecte jusqu'à leur destruction.

3. Définitions

Renseignement personnel

Tout renseignement qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier[1] (lieu de résidence, numéro de téléphone ou de cellulaire, adresse courriel, niveau de scolarité, numéro d'assurance sociale, date de naissance, etc.).

[1] *Loi sur l'accès*, article 54

Renseignement personnel sensible

Un renseignement personnel est sensible lorsque, par sa nature (notamment médicale, biométrique ou autrement intime) ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'attente raisonnable en matière du droit au respect de la vie privée[2].

Renseignement personnel sensible à caractère public

Le renseignement personnel qui a un caractère public en vertu de la loi n'est pas visé par la présente politique. Il concerne notamment l'exercice par la personne concernée d'une fonction au sein d'une entreprise ou d'un organisme public (nom, titre et fonction, coordonnées professionnelles (adresse, courrier électronique et numéro de téléphone de son lieu de travail[3])).

Incident de sécurité ou de confidentialité

L'accès, l'utilisation ou la communication non autorisés par la loi d'un renseignement personnel, la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.

Cycle de vie de l'information

L'ensemble des étapes visant le traitement d'un renseignement personnel à partir de sa création ou de sa collecte, en passant par son enregistrement, sa communication, sa consultation, son traitement et sa transmission jusqu'à sa conservation ou sa destruction en conformité avec le calendrier de conservation du Ministère.

4. Cadre réglementaire

La Politique est appliquée et interprétée en fonction des lois, des règlements et des directives gouvernementales en vigueur au Québec, notamment :

- *La Charte des droits et libertés de la personne* (chapitre C-12);
- Le *Code civil du Québec* (CCQ-1991);
- La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (chapitre A-2.1) (*Loi sur l'accès*);
- *La Loi sur les archives du Québec* (chapitre A-21.1);
- La *Loi concernant le cadre juridique des technologies de l'information* (chapitre C-1.1);
- La *Loi facilitant la divulgation d'actes répréhensibles à l'égard des organismes publics* (chapitre D-11.1);
- La *Loi sur les services de garde éducatifs à l'enfance* (chapitre S-4.1.1);

[2] *Loi sur l'accès*, article 59
[3] Idem, article 55

- Le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels* (chapitre A-2.1, r. 2);
- Le *Règlement sur l'éthique et la discipline dans la fonction publique* (chapitre F-3.1.1, r. 3);
- La politique et le cadre de gestion ministériels de la sécurité de l'information.
- La politique ministérielle sur la gestion des documents du ministère de la Famille, mai 2022.

5. Rôles et responsabilités

Chaque unité administrative est responsable des renseignements personnels qu'elle détient, et il est de la responsabilité de tous ses membres, internes et externes, de s'assurer du respect des obligations législatives et réglementaires ainsi que des procédures et directives internes qui les concernent.

Membres du personnel et ressources externes

Tout membre du personnel et toute ressource externe doivent respecter la présente politique et les règles de protection des renseignements personnels, notamment :

- accéder uniquement aux renseignements personnels nécessaires à l'exercice de leurs attributions et assurer le respect des mesures de protection applicables à ces renseignements;
- aviser sans délai son gestionnaire et, selon les processus mis en place au Ministère, la Direction de la cybersécurité et des solutions de soutien (DCSS) ou le bureau de l'accès aux documents et de la protection des renseignements personnels (bureau de l'accès) s'il a des motifs de croire que s'est produit un incident de sécurité ou de confidentialité;
- consulter le bureau de l'accès pour l'élaboration de sondages ou pour toute autre question relative à la protection de renseignements personnels;
- informer le bureau de l'accès de toute nouvelle communication ou de toute collecte de renseignement personnel envisagée et appliquer les recommandations formulées (ex. : formulaire Web);
- diriger toute demande d'accès à l'information venant de tiers ou de citoyen vers la répondante ministérielle de l'accès.

Gestionnaires

À titre de responsables des renseignements personnels détenus par leur unité administrative, les gestionnaires assurent le respect des obligations du Ministère et veillent à une saine gestion des données en leur possession. Ils doivent notamment :

- faire respecter les mesures de sécurité mises en place par le Ministère pour assurer la protection des renseignements personnels tout au long de leur cycle de vie;
- voir à la gestion conjointe avec la DCSS et le bureau de l'accès de tout incident de sécurité ou de confidentialité relativement aux renseignements personnels dont il a la responsabilité;

- mettre en place des processus permettant que les renseignements personnels utilisés soient à jour, exacts et complets pour servir aux fins pour lesquelles ils sont collectés ou utilisés;
- obtenir les consentements requis avant la collecte de tout renseignement personnel nécessaire à l'exercice des fonctions qui leur sont confiées et s'assurer que ceux-ci sont utilisés uniquement aux fins prévues et pour la durée requise;
- collaborer avec la répondante ministérielle à l'accès et le Comité AIPRP dans le cadre de leurs rôles et responsabilités (inventaire des fichiers de renseignements personnels, tenue des registres, reddition de comptes et autres obligations légales);
- aviser le Comité sur l'accès à l'information et la protection des renseignements personnels (Comité AIPRP) de tout projet mis en œuvre dans leur secteur et qui implique des renseignements personnels, notamment ceux d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services qui collecte, utilise, conserve, communique ou détruit des renseignements personnels;
- collaborer au processus d'analyse des plaintes sur la protection des renseignements personnels et mettre en œuvre les recommandations.

Direction de la cybersécurité et des solutions de soutien (DCSS)

- Rattachée à la Direction générale de la transformation numérique, la DCSS s'assure de la sécurité et de la confidentialité des données des actifs informationnels. Responsable de l'offre de service en matière de services infonuagiques, elle veille à la mise en place, à l'évolution et à la disponibilité des infrastructures technologiques. Elle assiste également les utilisateurs dans le traitement de leurs demandes.

Bureau de l'accès aux documents et de la protection des renseignements personnels (bureau de l'accès)

- Le bureau de l'accès conseille les membres de l'organisation relativement aux exigences de la *Loi sur l'accès* et veille à ce que des mesures de protection appropriées soient en place afin d'atténuer ou d'éliminer les risques d'utilisation ou de divulgation inappropriée de renseignements. Il est rattaché à la Direction du bureau de la sous-ministre et relève de sa directrice et répondante ministérielle de l'accès aux documents.

Comité sur l'accès à l'information et la protection des renseignements personnels (Comité AIPRP)

Le Comité AIPRP, qui relève de la sous-ministre de la Famille, est chargé de soutenir l'organisation dans l'exercice de ses responsabilités et dans l'exécution de ses obligations en vertu de la *Loi sur l'accès*. Il exerce un rôle de leadership et contribue à la promotion d'une culture organisationnelle qui renforce la protection des renseignements personnels et favorise la transparence. Ses membres doivent notamment :

- approuver les règles de gouvernance à l'égard des renseignements personnels;

- être consultés dès le début du projet, aux fins de l'évaluation des facteurs relatifs à la vie privée, sur tous les projets d'acquisition, de développement et de refonte d'un système d'information ou d'une prestation électronique de services impliquant des renseignements personnels;
- formuler un avis ou suggérer, à chacune des étapes d'un projet, des mesures de protection afin notamment d'atténuer les impacts sur l'atteinte à la vie privée et d'éliminer les risques quant à la sécurité ou à l'intégrité de l'information;
- s'assurer de la réalisation d'activités de formation relativement à l'accès aux documents et à la protection des renseignements personnels;
- évaluer annuellement le niveau de protection des renseignements personnels.

Le comité se compose de la personne responsable de l'accès aux documents, de celle responsable de la protection des renseignements personnels et de toute autre personne dont l'expertise est requise, y compris, le cas échéant, le responsable de la sécurité de l'information et le responsable de la gestion documentaire.

Répondante ministérielle de l'accès et de la protection des renseignements personnels (répondante ministérielle de l'accès)

Cette personne est déléguée par la sous-ministre de la Famille et exerce de manière autonome les fonctions de répondante de l'accès à l'information et de la protection des renseignements personnels conformément à ce que prévoit l'article 8 de la *Loi sur l'accès*. Elle protège le droit à l'information de toute personne (physique ou morale) ainsi que celui du respect de la vie privée.

Sous-ministre

La sous-ministre veille à assurer le respect et la mise en œuvre de la *Loi sur l'accès* à titre de personne ayant la plus haute autorité au sein de l'organisation. Elle peut déléguer à un membre du personnel de direction ces fonctions en matière d'accès à l'information et de renseignements personnels, en tout ou en partie.

6. Principes directeurs

Le Ministère est responsable des renseignements personnels qu'il détient, y compris ceux dont la collecte, l'utilisation, la conservation ou la destruction est assurée par un tiers. Il met en œuvre des politiques et des pratiques qui démontrent cette responsabilité.

Tous les employés et toutes les employées du Ministère ayant accès à des renseignements personnels sont interpellés et doivent se conformer aux obligations de l'organisation en matière de protection des renseignements. Les personnes qui agissent en tant que consultants externes ont également le devoir de respecter ses consignes.

La répondante ministérielle de l'accès veille à l'application de la Politique et s'assure que le personnel du Ministère en connaît les objectifs et s'y conforme. Les membres du Comité AIPRP l'appuient dans ses démarches.

Traitement des renseignements personnels

La protection des renseignements personnels est assurée tout au long de leur cycle de vie dans le respect des principes suivants :

La collecte :

Le Ministère ne collecte que les renseignements personnels qui sont nécessaires à l'exercice de ses attributions ou à la mise en œuvre d'un programme dont il a la gestion, sous réserve des exceptions prévues par la *Loi sur l'accès*.

Lorsqu'il collecte des renseignements personnels, le Ministère s'assure d'obtenir un consentement valide de la personne concernée, respectant les critères prévus à l'article 53.1 de la *Loi sur l'accès*. Ce consentement doit être demandé en termes simples et clairs, être manifeste et libre de toute contrainte, et donné à des fins précises pour une durée déterminée.

De plus, le Ministère s'assure que le consentement est obtenu de façon expresse dès que le renseignement personnel concerné est sensible, c'est-à-dire lorsque par sa nature ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'attente raisonnable en matière de vie privée.

L'utilisation :

Le Ministère limite l'utilisation des renseignements personnels aux seules fins pour lesquelles la personne concernée a été informée lors de la collecte ou pour lesquelles elle a consenti, à moins que la loi l'autorise à faire autrement. Il conserve les renseignements seulement pour la durée nécessaire pour accomplir les fins déterminées, sous réserve des règles prévues dans son calendrier de conservation.

La communication :

L'accès aux renseignements personnels au sein du Ministère est accordé aux seules personnes ayant qualité pour les recevoir et seulement lorsque ces renseignements personnels sont nécessaires à l'exercice de leurs fonctions.

Lorsque des renseignements personnels sont communiqués à un tiers ou à un autre organisme, le Ministère s'assure que :

- la personne concernée consent à cette communication, à moins que cette utilisation ne soit autrement autorisée par la *Loi sur l'accès*;
- les mesures de sécurité sont convenues dans le cadre d'une entente avec l'organisme public concerné ou précisées dans le contrat avec le tiers, lorsqu'applicable;

- les renseignements sont communiqués de manière sécuritaire, par exemple au moyen d'une plateforme d'échange ou d'un courriel sécurisé;
- cette communication est inscrite dans le registre approprié, lorsque requis.

Si des renseignements personnels sont communiqués à des fournisseurs de services ou que ces renseignements sont nécessaires à une prestation de services, le Ministère s'assure que cette communication est faite dans le cadre d'un contrat ou d'une entente écrite qui stipule clairement les exigences relatives aux mesures qui doivent être prises pour protéger les renseignements communiqués. Cet engagement les oblige notamment à garder les renseignements personnels confidentiels, à les utiliser uniquement aux fins pour lesquelles le Ministère les divulgue et à les traiter selon les normes énoncées et dans le respect des lois.

La conservation et la protection :

Le Ministère respecte les normes de sécurité de l'information fixées par le gouvernement du Québec afin de protéger les renseignements personnels détenus pendant toute la durée de leur conservation, en s'assurant qu'elles sont raisonnables, compte tenu notamment de leur sensibilité et du contexte de leur utilisation.

Le Ministère révise périodiquement ces mesures de sécurité pour s'assurer qu'elles sont bien appliquées, qu'elles sont encore pleinement efficaces et qu'elles conviennent toujours compte tenu de l'évolution de ses systèmes et des technologies de l'information.

Les renseignements personnels sont conservés tant et aussi longtemps qu'ils sont nécessaires pour mener les activités et offrir des services aux personnes concernées. Ils sont, par la suite, conservés pendant la période supplémentaire prévue aux règles de conservation approuvées par Bibliothèque et Archives nationales du Québec, le cas échéant.

La destruction :

Le Ministère détruit de façon sécuritaire les renseignements personnels lorsque les fins pour lesquelles ils ont été recueillis sont accomplies conformément à l'article 73 de la *Loi sur l'accès*, sous réserve des lois applicables quant à leur conservation.

Lorsqu'il procède à la destruction de documents contenant des renseignements personnels, le Ministère s'assure de prendre les mesures de protection nécessaires visant à assurer la confidentialité de ceux-ci. La méthode de destruction utilisée doit être déterminée en fonction de la sensibilité des renseignements, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support.

7. Évaluation des facteurs relatifs à la vie privée

Le Ministère procède à une évaluation des facteurs relatifs à la vie privée avant de communiquer un renseignement personnel à l'extérieur du Québec (ex. : dans le cadre de télétravail, contrat en infonuagique), et ce, pour tout projet d'acquisition, de développement ou de refonte d'un système

d'information ou d'une prestation électronique de services qui impliquerait la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels.

Les directions concernées doivent remplir le formulaire d'évaluation des facteurs relatifs à la vie privée préparé à cet effet et le transmettre pour analyse et recommandations à la répondante ministérielle de l'accès à l'adresse suivante : accesinformation@mfa.gouv.qc.ca.

8. Droits d'accès et de rectification

Toute personne a le droit d'accéder aux renseignements personnels détenus à son égard par le Ministère et de les faire rectifier en cas d'inexactitude dans la mesure prévue par la loi.

Une demande ne peut être considérée que si elle est faite par écrit par une personne physique confirmant son identité à titre de personne concernée. Cette demande doit être adressée par courriel à la responsable ministérielle de l'accès, à l'adresse suivante : accesinformation@mfa.gouv.qc.ca.

Les dispositions prévues dans la *Loi sur l'accès* s'appliquent.

9. Processus de traitement des plaintes

Le dépôt de la plainte

Toute personne à l'égard de laquelle le Ministère détient des renseignements personnels, y compris les membres de son personnel, peut transmettre une plainte par écrit auprès de la répondante ministérielle de l'accès.

La plainte doit être formulée à accesinformation@mfa.gouv.qc.ca et contenir les renseignements suivants :

- le nom de la personne plaignante;
- les coordonnées pour la joindre;
- les motifs et les faits au soutien de la plainte.

Le traitement de la plainte

Toute plainte relative à la protection des renseignements personnels est transmise à la répondante ministérielle de l'accès qui l'analyse et s'assure de son traitement si celle-ci est recevable.

Elle fait les vérifications qui s'imposent auprès des personnes ou des unités administratives visées et, lorsque requis, elle peut recommander les mesures et les actions nécessaires pour corriger la situation ou éviter que des situations semblables se reproduisent.

Au terme du processus, une réponse finale est transmise à la personne qui a formulé la plainte.

10. Gestion des incidents de confidentialité

Lorsque le Ministère a des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel qu'il détient, il prend les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent.

Si l'incident de confidentialité présente le risque qu'un préjudice sérieux soit causé, le Ministère en avise la Commission d'accès à l'information du Québec avec diligence. Il avise également toute personne susceptible de prévenir ou de diminuer le risque de préjudice sérieux et toute personne dont un renseignement personnel est concerné par l'incident.

Le Ministère tient un registre des incidents de confidentialité, dont le contenu est déterminé par la *Loi sur l'accès*.

11. Sondages

Toute unité administrative du Ministère doit consulter le Comité AIPRP afin d'obtenir un avis sur les mesures particulières à respecter en matière de protection des renseignements personnels relativement aux sondages recueillant ou utilisant des renseignements personnels, que ceux-ci soient réalisés par le Ministère ou par un tiers qui agit pour son compte.

Le Comité AIPRP s'assurera notamment :

- de la nécessité de recourir au sondage;
- du fait que les renseignements personnels recueillis sont nécessaires à la réalisation des fins déterminées;
- de l'obtention du consentement valide selon les critères prévus à l'article 53.1 de la *Loi sur l'accès*;
- de la prise de mesures de protection à l'égard des renseignements personnels recueillis ou utilisés;
- de l'aspect éthique de l'activité compte tenu, notamment, de la nature du sondage, des personnes visées, de la sensibilité des renseignements personnels recueillis et de la finalité de l'utilisation de ceux-ci.

Un formulaire prévu à cette fin et disponible sur l'intranet doit être rempli et transmis par l'unité administrative responsable du sondage au bureau de l'accès, à l'adresse suivante : accesinformation@mfa.gouv.qc.ca.

Une directive sur les sondages est également en vigueur au sein du Ministère. Elle peut être consultée dans la section Accès information de l'intranet.

12. Activités de formation et de sensibilisation

Le Ministère offre à son personnel des activités de formation et de sensibilisation. Il met également à sa disposition des outils qui lui permettent de se conformer à ses obligations législatives. Parmi ceux-ci, notons :

- une formation présentant les principes en matière d'accès à l'information et de protection des renseignements personnels;
- divers outils, gabarits, aide-mémoire applicables à différents aspects de l'encadrement relativement à l'accès à l'information et à la protection des renseignements personnels (disponibles sur le site intranet du Ministère);
- des rencontres avec les membres du réseau des répondants en matière d'accès;
- des capsules de sensibilisation et d'invitation à l'autoformation en ligne (proposées par la Direction de la cybersécurité et des solutions de soutien);
- un rappel des consignes à mettre en application lors de l'utilisation, le classement et la destruction de documents analogiques (papier) et numériques contenant des renseignements personnels lors des rencontres de formation ainsi que dans les capsules d'autoformation en ligne en gestion des documents (DGICD).
- de la sensibilisation lors des activités d'accueil du personnel.

Entrée en vigueur et révision de la politique

La Politique est approuvée par le Comité AIPRP, conformément à l'article 63.3 de la *Loi sur l'accès*. Elle demeure en application tant et aussi longtemps qu'elle n'est pas abrogée, modifiée ou remplacée par une autre politique.

Toute question en lien avec la Politique doit être adressée par courriel à la répondante ministérielle de l'accès, à l'adresse suivante : accesinformation@mfa.gouv.qc.ca.

Famille
Québec

Politique de sécurité de l'information

Ministère de la Famille

Mars 2024

Votre gouvernement

Québec

Coordination et rédaction
Sous-ministériat au financement, aux infrastructures et à l'administration
Direction générale de la transformation numérique
Direction de la cybersécurité et des solutions de soutien
Centre de la cybersécurité et services infonuagiques

HISTORIQUE

Révision	Date	Description du changement
0.1	2014-03-14	Version initiale
0.2	2023-12-07	Modification au document à la suite de l'émission des nouvelles exigences gouvernementales
1.0	2024-03-27	Modifications du document à la suite d'ajustements

Table des matières

1 Préambule

Le ministère de la Famille (Ministère), par la nature de ses activités, doit collecter, échanger, traiter, sauvegarder et supprimer de l'information. Ces informations peuvent revêtir, dans certains cas un caractère stratégique, sensible ou confidentiel. Il est donc important qu'une protection appropriée de cette information soit mise en place.

La présente politique met en exergue l'engagement du Ministère à la mise en œuvre d'un cadre de gouvernance en sécurité de l'information, et ce, en conformité aux lois, règlements, directives et normes en vigueur : Loi sur la gouvernance et la gestion des ressources informationnelles (LGGRI), Directive gouvernementale sur la sécurité de l'information.

Celle-ci a pour objet d'assurer adéquatement une prise en charge globale de la sécurité des ressources informationnelles que le Ministère détient ou utilise dans l'exercice de ses fonctions, même lorsque la conservation de l'information est assurée par un tiers.

Un cadre de gestion accompagne cette politique et précise les rôles et responsabilités des différents intervenants en matière de sécurité de l'information.

2 Définitions

CERT/AQ (Computer Emergency Response Team I Administration québécoise) : sigle de l'équipe de réponse aux incidents de sécurité de l'information du Gouvernement du Québec appartenant au Centre gouvernemental de cyberdéfense (CGCD).

Confidentialité : propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées et de n'être divulguée qu'à celles-ci.

Continuité des services : capacité d'une organisation d'assurer, en cas de sinistre, la poursuite de ses processus d'affaires selon le niveau de service prédéfini.

Cycle de vie de l'information : ensemble des étapes que franchit une information à partir de sa création en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission jusqu'à sa conservation ou sa destruction.

Disponibilité : propriété d'une information d'être accessible en temps voulu et de la manière requise pour une personne autorisée.

GMVI : processus de gestion des évènements liés à des menaces, des vulnérabilités et des incidents de sécurité de l'information.

Information : ensemble de données ayant un sens. L'information est un élément de connaissance (voix, donnée, image) susceptible d'être conservé, traité ou transmis à l'aide d'un support et d'un mode de codification normalisé.

Intégrité : propriété d'une information de ne subir aucune altération accidentelle ou non autorisée lors de leur traitement, de leur transmission ou de leur conservation.

Ressources informationnelles : ensemble de ressources apportant des éléments d'information et qui sont utilisées par une organisation pour mener à bien sa mission. Les ressources informationnelles incluent notamment les ressources humaines, matérielles, financières et technologiques.

Renseignement personnel : tout renseignement qui concerne une personne physique et qui permet directement ou indirectement de l'identifier. Un renseignement personnel qui a un caractère public en vertu d'une loi n'est pas considéré comme un renseignement personnel aux fins de la politique de sécurité (source : Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels).

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 organisation.

3 Objectif de la politique

La présente Politique a pour objectif d'affirmer l'engagement du Ministère de s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information, quel que soit son support ou son moyen de communication. Plus précisément, il s'agit d'assurer, tout au long du cycle de vie de l'information, sa disponibilité, son intégrité et sa confidentialité.

4 Champ d'application

4.1 Les informations visées

Cette politique s'applique aux ressources informationnelles suivantes :

- Ressources informationnelles appartenant au Ministère et exploitées par celui-ci;
- Ressources informationnelles appartenant au Ministère et exploitées ou détenues par un partenaire, un fournisseur de produits et services ou un tiers;

- Ressources informationnelles appartenant à un tiers et utilisées par le Ministère dans le cadre de ses échanges avec ses mandataires.

La sécurité de l'information doit être assurée, quel que soit son support ou mode de transmission. Ainsi, cette politique s'applique tout autant pour l'information consignée sur des documents papiers que numériques ou communiquée par tout moyen.

4.2 Les personnes visées

Cette politique s'adresse à tout le personnel du Ministère ainsi qu'à toute personne ayant accès aux ressources informationnelles du Ministère (partenaires, fournisseurs de produits et services ou tiers impliqués dans la prestation de services du Ministère sur site ou à distance (infonuagique)).

4.3 Les activités visées

Toutes les activités impliquant la création, l'utilisation, le traitement, la communication ou la conservation de l'information sous toutes ses formes et tout au long de son cycle de vie sont visées par la présente politique, que celles-ci soient conduites dans les locaux du Ministère ou dans un autre lieu.

5 Principes directeurs

Les orientations et principes stratégiques en sécurité de l'information du ministère de la Famille sont en adéquation et en conformité avec la directive gouvernementale de la sécurité de l'information.

Plus précisément, il s'agit d'assurer, tout au long du cycle de vie de l'information, sa disponibilité, son intégrité et sa confidentialité.

5.1 Pérennité

La Sécurité de l'information doit être durable et garantir à long terme la continuité des opérations du Ministère.

5.2 Éthique

La sécurité de l'information doit être guidée par des principes éthiques clairs qui protègent les droits des utilisateurs et respectent les lois et normes en vigueur tout en visant à assurer la régulation des conduites et la responsabilisation individuelle.

5.3 Évolution

La sécurité de l'information doit être adaptative et évolutive pour faire face aux menaces et aux risques en constante évolution.

Les pratiques et les solutions retenues en matière de sécurité de l'information doivent être réévaluées périodiquement et actualisées afin de tenir compte des changements juridiques, organisationnels, humains et technologiques.

5.4 Responsabilité et imputabilité

Les responsabilités en matière de sécurité de l'information sont attribuées clairement à tous les niveaux du Ministère ainsi que de ses partenaires.

5.5 Transparence et universalité

L'information concernant les événements, les processus et les mesures de sécurité de l'information doit être transparente et accessible à tous les utilisateurs et parties prenantes concernées, sous réserve du droit applicable (dans certains cas, vu le risque, l'information peut être confidentielle et n'être accessible qu'aux personnes ou entités désignées et autorisées).

Les pratiques et les solutions retenues en matière de sécurité de l'information doivent correspondre, dans la mesure du possible, à des façons de faire reconnues et généralement utilisées au sein de l'appareil gouvernemental québécois ou à l'échelle nationale et internationale.

6 Énoncés de sécurité

Les énoncés suivants constituent les orientations stratégiques et la vision d'encadrement de la sécurité de l'information que se donne le ministère de la Famille.

6.1 Assurer la protection de l'information durant tout son cycle de vie

Le Ministère adhère aux orientations et aux objectifs stratégiques gouvernementaux en matière de sécurité de l'information et s'engage à ce que les pratiques et les solutions retenues en la matière correspondent à des façons de faire reconnues et généralement utilisées à l'échelle nationale et internationale.

Le Ministère reconnaît que les actifs informationnels qu'il détient sont essentiels à ses activités courantes et, de ce fait, doivent faire l'objet d'une utilisation appropriée, d'une protection adéquate et d'une évaluation régulière en procédant à des révisions des accès et des audits. Le niveau de protection dont

les actifs informationnels doivent faire l'objet est établi en fonction de leur importance, de leur confidentialité et des risques d'accident, d'erreur et de malveillance auxquels ils sont exposés.

La sécurité des actifs informationnels est soutenue par une démarche d'éthique visant à assurer la régulation des conduites et la responsabilisation individuelle.

6.2 Protection des renseignements confidentiels

Toute information confidentielle doit être préservée de toute divulgation, de tout accès ou de toute utilisation non autorisée ou illicite. Sont notamment considérés comme confidentiels au sens de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, les renseignements personnels, ainsi que tout renseignement dont la divulgation aurait des incidences néfastes, notamment sur les relations intergouvernementales, les négociations entre organismes publics, l'économie, les tiers relativement à leurs renseignements industriels, financiers, commerciaux, scientifiques ou techniques, l'administration de la justice et la sécurité publique, les décisions administratives ou politiques et la vérification.

6.3 Sensibilisation et formation

Le Ministère s'engage, sur une base régulière, à sensibiliser et à former le personnel du Ministère à la sécurité de l'information, aux conséquences d'une atteinte à sa sécurité ainsi qu'à son rôle et ses obligations en cette matière.

6.4 Droit de regard et d'intervention

Le Ministère exerce, en conformité avec la législation et la réglementation en vigueur, un droit de regard et d'intervention sur l'utilisation qui est faite de toute information ou technologie de l'information en sa possession, et ce, pour quiconque y ayant accès.

7 Obligations des intervenants clés en matière de sécurité de l'information

La présente politique fixe les obligations en matière de sécurité de l'information, attribuées, notamment, au sous-ministre, chef délégué de la sécurité de l'information (CDSI), répondants en matière de sécurité de l'information, détenteurs de l'information, gestionnaires d'entités administratives, utilisateurs.

a) **Le sous-ministre :** est le premier responsable de la sécurité de l'information au sein du Ministère. À ce titre, il s'assure du respect des lois, des règlements, des directives et des politiques mentionnés à l'annexe 2 de ce document.

b) **Le chef délégué de la sécurité de l'information (CDSI) :** assure la protection des ressources informationnelles et de l'information, notamment par la gestion des risques et des vulnérabilités, ainsi que par la mise en œuvre de mesures visant à les protéger de toute forme d'atteinte, telles des menaces ou des cyberattaques.

c) **Les détenteurs de l'information :** un employé désigné par le Ministère et inscrit au registre d'autorité, appartenant à la classe d'emploi de niveau-cadre ou à une classe d'emploi de niveau supérieur, et dont le rôle est, entre autres, de s'assurer de la sécurité de l'information et des ressources qui la sous-tendent, relevant de la responsabilité de son unité administrative.

d) **Les gestionnaires :** sont chargés de la mise en œuvre des dispositions de la présente politique auprès du personnel relevant de leur autorité.

e) **Les utilisateurs :** les personnes qui utilisent les ressources informationnelles doivent se conformer aux directives gouvernementales (voir annexe 2), à la présente politique et aux règles qui leur sont applicables, en acceptant la déclaration d'engagement quant au respect des règles de sécurité de l'information lors de leur arrivée ou lors de leur évaluation annuelle (annexe 3).

f) **Ministère de la Cybersécurité et du Numérique (MCN) :** le MCN, dans le cadre de l'entente en plan avec le Ministère, joue un rôle clé pour assurer la sécurité de l'information au sein du Ministère. Sa responsabilité majeure englobe la conception, la mise en œuvre, la maintenance de l'infrastructure technologique et la gestion des incidents de sécurité concernant cette infrastructure.

g) **Audit interne:** l'audit interne procure au Ministère une assurance sur le degré de maîtrise de ses opérations, lui apporte des conseils et contribue à créer de la valeur ajoutée.

8 Obligations des utilisateurs

Tout utilisateur a l'obligation de protéger les actifs informationnels mis à sa disposition par le Ministère. À cette fin, il doit :

a) prendre connaissance de la présente Politique, des directives, des procédures et autres lignes de conduite en découlant, y adhérer et prendre l'engagement de s'y conformer en signant annuellement la déclaration d'engagement;

b) être responsable de l'intégrité, de la sécurité de l'information et des traitements effectués sur l'équipement qu'il utilise, ainsi que des activités qui résultent de l'usage de ses codes d'utilisateur et de ses mots de passe;

c) s'assurer de la confidentialité des renseignements qu'il détient, peu importe qu'il soit un employé, un consultant, un partenaire, un client ou un fournisseur du Ministère;

d) utiliser, à l'intérieur des droits d'accès qui lui sont attribués et uniquement lorsqu'ils sont nécessaires à l'exercice de ses fonctions, les actifs informationnels mis à sa disposition en se limitant aux fins auxquelles ils sont destinés;

e) respecter les mesures de sécurité mises en place sur son poste de travail et sur tout équipement contenant des données à protéger et ne pas modifier leur configuration ni les désactiver;

f) se conformer aux exigences légales sur l'utilisation de produits, de documents et d'information à l'égard desquels il pourrait y avoir des droits de propriété intellectuelle;

g) signaler immédiatement à son gestionnaire 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 du Ministère;

h) remettre les différentes cartes d'identité et d'accès, les actifs informationnels ainsi que tout l'équipement informatique ou de téléphonie mis à sa disposition dans le cadre de ses fonctions au moment de son départ du Ministère.

9 Sanctions

Toute personne contrevenant à la présente politique ou aux directives en découlant, s'expose à des mesures disciplinaires, administratives ou légales en fonction de la gravité de son geste. Ces mesures peuvent inclure la suspension des privilèges, la réprimande, la suspension, le congédiement ou autre, et ce, conformément aux dispositions des conventions collectives, des ententes ou des contrats.

Le Ministère peut transmettre à toute autorité judiciaire les renseignements colligés et qui le portent à croire qu'une infraction à toute loi ou tout règlement en vigueur a été commise.

10 Dispositions finales

a) Le sous-ministre approuve la présente politique.

b) La présente politique entre en vigueur à sa date d'approbation et remplace toute version antérieure.

c) Le CDSI est chargé de la mise en œuvre des dispositions de la présente politique.

La présente politique doit être révisée lors de changements législatifs, administratifs, réglementaires ou technologiques significatifs affectant sa mise en application.

Document approuvé par la sous-ministre

[redacted]

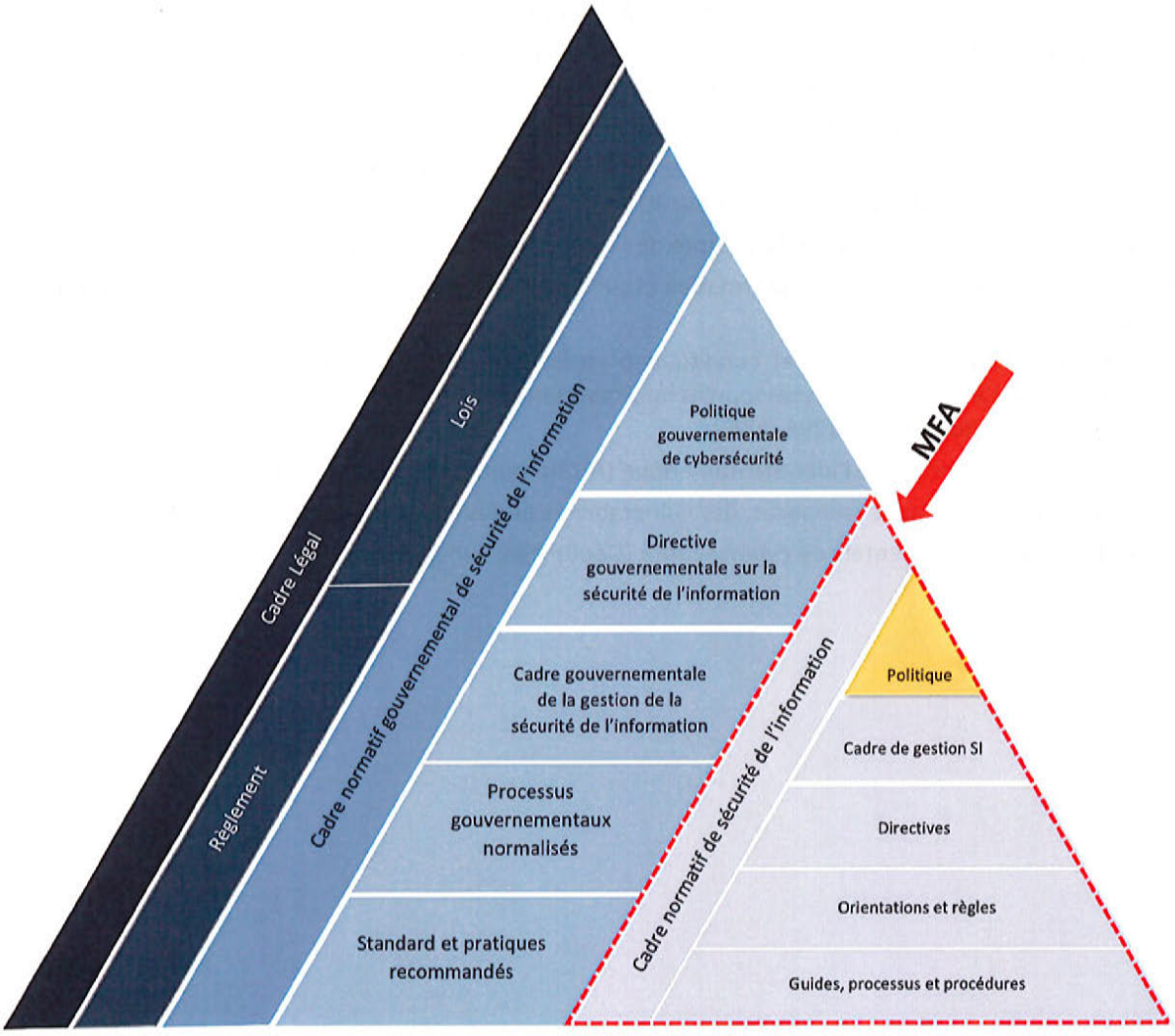
Date : 26 avril 2024

Mme Julie Blackburn

Annexe 1

Représentation graphique du cadre normatif gouvernemental de sécurité de l'information

La représentation graphique suivante présente le positionnement et l'engagement du Ministère envers le cadre normatif de sécurité de l'information du gouvernement. Cette dernière, comprend la politique de gestion de la sécurité de l'information.



Annexe 2

Documents de références

- Charte des droits et libertés de la personne (RLRQ, chapitre C-12);
- Code civil du Québec (RLRQ);
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A- 2.1);
- Loi concernant le cadre juridique des technologies de l'information (RLRQ, chapitre C-1.1);
- Loi sur la fonction publique (RLRQ, chapitre F-3.1.1);
- Loi sur le ministère de la Cybersécurité et du Numérique (RLRQ, chapitre M-17.1.1)
- Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, chapitre G-1.03);
- Règlement sur l'éthique et la discipline dans la fonction publique (RLRQ, chapitre F-3.1.1, r. 3);
- Cadre gouvernemental de gestion de la sécurité de l'information arrêtée numéro 2022-04 du MCN en date du 26 juillet 2022 (Entrée en vigueur 10 août 2022);
- Directive gouvernementale sur la sécurité de l'information (Décret 1514-2021);
- Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1, r.2);
- Règlement sur les modalités et conditions d'application des articles 12.2 à 12.4 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (Décret 1296-2022);
- Règles sur l'assurance de l'identité numérique (Arrêté numéro 2022-05 du MCN);
- Processus de gestion des menaces, des vulnérabilités et des incidents, version 4.2 du 22-06-2022;
- Politique gouvernementale de cybersécurité (Dépôt légal – mars 2020).

Annexe 3

Déclaration d'engagement par les utilisateurs quant au respect des règles de sécurité de l'information

Les utilisateurs ont l'obligation de protéger les actifs informationnels mis à leur disposition par le ministère. À cette fin, ils doivent :

a) se conformer aux directives gouvernementales, à la politique sur la sécurité de l'information ainsi qu'aux directives sectorielles, aux procédures et aux autres lignes de conduite se rapportant à la sécurité de l'information du Ministère;

b) s'assurer de la confidentialité des renseignements qu'il détient;

c) utiliser, à l'intérieur des droits d'accès qui lui sont attribués et uniquement lorsqu'ils sont nécessaires à l'exercice de ses fonctions, les actifs informationnels mis à sa disposition en se limitant aux fins auxquelles ils sont destinés;

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

e) se conformer aux exigences légales sur l'utilisation de produits, de documents et d'information à l'égard desquels il pourrait y avoir des droits de propriété intellectuelle;

f) signaler immédiatement à son gestionnaire 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 du Ministère;

g) remettre les différentes cartes d'identité et d'accès, les actifs informationnels ainsi que tout l'équipement informatique ou de téléphonie mis à sa disposition dans le cadre de ses fonctions au moment de son départ du Ministère.

Je soussigné(e), _____, reconnais avoir pris connaissance des règles, ci-dessus reproduites, sur la sécurité de l'information du ministère et m'engage à les respecter.

Famille
Québec

Cadre de gestion de la sécurité de l'information

Ministère de la Famille

Mars 2024

Votre gouvernement

Québec

Coordination et rédaction
Sous ministériat au financement, aux infrastructures et à l'administration
Direction générale de la transformation numérique
Direction de la cybersécurité et des solutions de soutien
Centre de la cybersécurité et services infonuagiques

Historique

Révision	Date	Description du changement
0.1	2015-02-13	Version initiale
0.2	2023-12-07	Modification au document à la suite de l'émission des nouvelles exigences gouvernementales
1.0	2024-04-04	Modification au document à la suite d'ajustements

Table des matières

1 Introduction

Le présent cadre vient en complément à la politique de sécurité de l'information. Il vise à renforcer la gouvernance de la sécurité de l'information du ministère de la Famille (Ministère) par la mise en place d'une structure organisationnelle de la sécurité de l'information et la définition des rôles et des responsabilités de divers intervenants.

Il est destiné à tout le personnel du Ministère, notamment aux intervenants et intervenantes en sécurité de l'information, ainsi qu'à ses partenaires, aux fournisseurs et prestataires de services qui assument une responsabilité directe ou indirecte en matière de sécurité de l'information au Ministère. Il contient une description exhaustive des rôles et responsabilités liés au volet stratégique, tactique et opérationnel.

1.1 Contexte

Le Cadre de gestion de la sécurité de l'information est élaboré en application de la Directive gouvernementale sur la sécurité de l'information. Celle-ci fait obligation au chef délégué de la sécurité de l'information de mettre en œuvre un cadre de gouvernance qui régit la sécurité de l'information.

1.2 Définitions

Actif informationnel : ensemble constitué d'informations, à l'exception des ressources humaines. L'actif informationnel peut inclure une banque d'information électronique, un système d'information, une technologie de l'information ou une installation, ou encore un ensemble de ces éléments acquis ou constitués par une organisation.

CERT/AQ (Computer Emergency Response Team I Administration québécoise) : sigle de l'équipe de réponse aux incidents de sécurité de l'information du Gouvernement du Québec appartenant au Centre gouvernemental de cyberdéfense (CGCD).

Confidentialité : propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées et de n'être divulguée qu'à celles-ci.

Continuité des services : capacité d'une organisation d'assurer, en cas de sinistre, la poursuite de ses processus d'affaires selon le niveau de service prédéfini.

Cycle de vie de l'information : ensemble des étapes que franchit une information à partir de sa création en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission jusqu'à sa conservation ou sa destruction.

Disponibilité : propriété d'une information d'être accessible en temps voulu et de la manière requise pour une personne autorisée.

GMVI : processus de gestion des évènements liés à des menaces, des vulnérabilités et des incidents de sécurité de l'information.

Information : ensemble de données ayant un sens. L'information est un élément de connaissance (voix, donnée, image) susceptible d'être conservé, traité ou transmis à l'aide d'un support et d'un mode de codification normalisé.

Intégrité : propriété d'une information de ne subir aucune altération accidentelle ou non autorisée lors de leur traitement, de leur transmission ou de leur conservation.

MVI : ce sont les menaces, les vulnérabilités et les incidents.

Renseignement personnel : tout renseignement qui concerne une personne physique et qui permet directement ou indirectement de l'identifier. Un renseignement personnel qui a un caractère public en vertu d'une loi n'est pas considéré comme un renseignement personnel aux fins de la politique de sécurité (source : Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels).

Ressources informationnelles : ensemble de ressources apportant des éléments d'information et qui est utilisé par une organisation pour mener à bien sa mission. Les ressources informationnelles incluent notamment les ressources humaines, matérielles, financières et technologiques.

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 organisation.

2 Organisation fonctionnelle de la sécurité de l'information

L'organisation fonctionnelle de la sécurité de l'information au sein de l'administration publique s'articule, dans le respect de la Loi et de la Directive, autour d'une structure de gouvernance qui repose sur trois niveaux de gestion :

- Un niveau gouvernemental;
- Un niveau de portefeuille;
- Un niveau organisationnel.

Une telle structure de gouvernance repose également sur la présence de liens fonctionnels entre les intervenants en matière de sécurité de l'information d'un niveau à l'autre, lesquels liens visent à favoriser une concertation agile et transparente pour répondre efficacement aux exigences de sécurité de l'information. Ces liens sont énoncés dans la Directive et représentés par des pointillés à la Figure 1 : Structure de gouvernance de la sécurité de l'information gouvernementale.

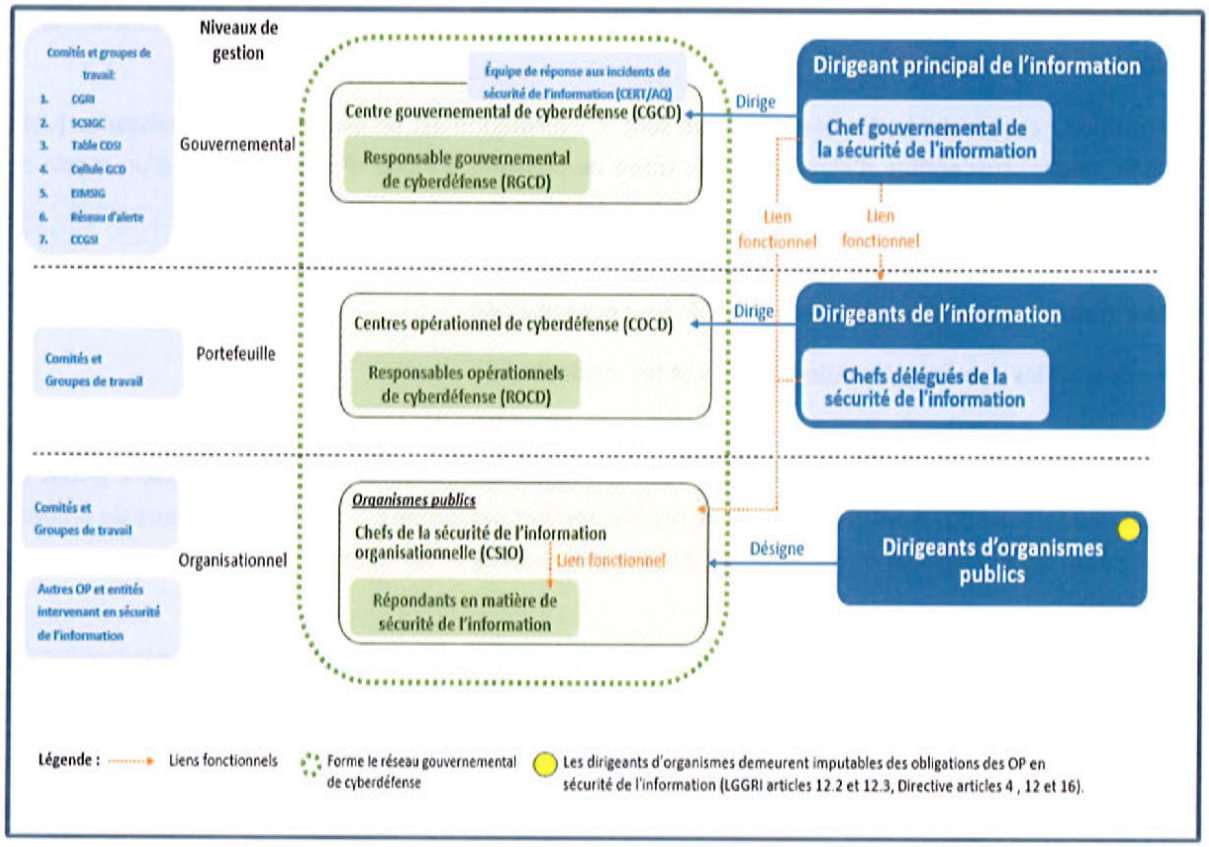


Figure 1 : Structure de gouvernance de la sécurité de l'information gouvernementale

Le présent document s'intéressera particulièrement aux paliers « Portefeuille » et « Organisationnel ». Pour obtenir plus de détails concernant l'organisation fonctionnelle de la sécurité de l'information au sein de l'administration publique, le lecteur peut consulter le Cadre gouvernemental de gestion de la sécurité de l'information.

3 Rôles et responsabilités

Les rôles et responsabilités décrits ci-après sont désignés pour assurer la mise en œuvre de la sécurité de l'information.

En plus des intervenants internes au Ministère, il est important de souligner le partenariat majeur du ministère de la Cybersécurité et du numérique (MCN) en termes de sécurité de l'information (détail en section 3.4).

3.1 Principaux intervenants

3.1.1 Sous-ministre

Le sous-ministre est le premier responsable de la sécurité de l'information. À ce titre, il s'assure du respect des lois, des règlements, des directives et des politiques mentionnés à l'annexe 1 de la Politique sur la sécurité de l'information du Ministère. À cet effet, il :

- assure le maintien du lien fonctionnel entre le chef de la sécurité de l'information organisationnelle, le chef délégué à la sécurité de l'information et le chef gouvernemental de la sécurité de l'information, avec les adaptations nécessaires;
- adopte et s'assure de la mise en œuvre des orientations stratégiques de la sécurité de l'information du Ministère, de la politique, du cadre de gestion, des directives et des plans d'action;
- approuve et présente lorsque requis, aux instances gouvernementales concernées, les bilans, les plans d'action et les programmes de rehaussement portant sur la sécurité de l'information;
- s'assure de la réalisation périodique d'audits de sécurité de l'information et de tests d'intrusions et de vulnérabilités, conformément aux obligations gouvernementales, et il en dégage les priorités d'actions ainsi que les échéanciers afférents;
- favorise l'utilisation des services communs de sécurité de l'information déterminés par le Conseil du trésor;
- s'assure que les ententes de service et les contrats, conclus avec les prestataires de services, les partenaires et les mandataires, stipulent des clauses garantissant le respect des exigences de sécurité de l'information;
- s'assure de la mise en place d'un programme formel et continu de formation et de sensibilisation du personnel en matière de sécurité de l'information;
- désigne les répondants pour des domaines spécifiques en matière de sécurité de l'information;
- peut nommer quelqu'un qui le représente pour présider certains comités (ex. : comité de crise ministériel, etc.)

3.1.2 Chef délégué de la sécurité de l'information (CDSI)

Le chef délégué de la sécurité de l'information assume, sous le lien fonctionnel du chef gouvernemental de la sécurité de l'information (CGSI), les responsabilités suivantes :

- mettre en œuvre un cadre de gouvernance qui régit la sécurité de l'information;

- diriger le Centre opérationnel de cyberdéfense auquel il se rattache, l'opérationnaliser en demandant, lorsqu'il le juge à propos, la contribution des organismes qui s'y rattachent, et contribuer à faire évoluer l'offre de services de ce centre;
- désigner, parmi les membres du personnel d'encadrement sous sa direction et conformément aux indications d'application du chef gouvernemental de la sécurité de l'information, un responsable opérationnel de cyberdéfense dont le rôle est de voir au bon fonctionnement du Centre opérationnel de cyberdéfense;
- mettre en œuvre toute action requise pour la prise en charge d'un événement de sécurité;
- élaborer, au besoin et dans un souci d'efficacité et de gestion performante des ressources informationnelles, des processus de sécurité de l'information, déployer les mesures afférentes et assurer le suivi de leur mise en œuvre;
- apporter le soutien et l'accompagnement requis en matière de sécurité de l'information, notamment par des conseils, des outils, des pratiques exemplaires de sécurité de l'information ainsi que par le développement des compétences et la sensibilisation du personnel affecté en la matière ou par toute autre mesure jugée nécessaire;
- mettre en place les comités ou les groupes de travail appropriés de concertation en matière de sécurité de l'information et en assurer la coordination.

3.1.3 Chef de la sécurité de l'information organisationnelle (CSIO)

Le chef de la sécurité de l'information organisationnelle assume la responsabilité de la prise en charge globale de la sécurité de l'information au sein du Ministère. Il travaille en étroite collaboration avec les répondants en matière de sécurité de l'information pour assurer la prise en charge des exigences de sécurité de l'information. Il assume, dans l'organisation fonctionnelle de la sécurité de l'information, les responsabilités suivantes :

- mettre en œuvre les décisions émanant du chef gouvernemental de la sécurité de l'information et du chef délégué de la sécurité de l'information auquel il se rattache, notamment les indications d'application et les indications d'application particulières, en coordonner l'exécution et veiller à leur application;
- contribuer à la mise en œuvre du cadre de gouvernance qui régit la sécurité de l'information au sein du Ministère;
- contribuer à la mise en œuvre des processus gouvernementaux normalisés en matière de gestion de la sécurité de l'information et des processus de sécurité de l'information élaborés par le chef délégué de la sécurité de l'information;

- s'assurer de la prise en charge des exigences de sécurité de l'information lors de la réalisation de projets de développement, d'acquisition, d'évolution ou de remplacement d'un actif informationnel ou d'un service en ressources informationnelles;
- aviser sans délai le chef délégué de la sécurité de l'information lorsqu'un événement de sécurité présente un risque qu'un préjudice sérieux soit causé;
- mettre en œuvre les actions requises pour la prise en charge d'un événement de sécurité;
- tenir un registre des événements de sécurité selon les exigences de la Directive et les modalités précisées par le chef délégué de la sécurité de l'information;
- fournir les informations demandées par le chef gouvernemental de la sécurité de l'information et le chef délégué de la sécurité de l'information auquel il se rattache relativement à la reddition de comptes, ou toute autre information requise par ces derniers;
- mettre en place au sein du Ministère les comités et les groupes de travail appropriés de concertation en matière de sécurité de l'information et en assurer la coordination;
- assurer le développement des compétences du personnel du Ministère en matière de sécurité de l'information.

3.1.4 Responsables opérationnels de cyberdéfense (ROCD)

Le responsable opérationnel de cyberdéfense assume, dans l'organisation fonctionnelle de la sécurité de l'information, les responsabilités suivantes :

- appuyer le chef délégué de la sécurité de l'information (CDSI) dans la direction, l'opérationnalisation et l'évolution de l'offre de service de son centre opérationnel de cyberdéfense (COCD);
- conseiller le chef délégué de la sécurité de l'information notamment, sur les orientations, les priorités d'action, les pratiques communes de cybersécurité, les mécanismes de reddition de comptes et sur l'optimisation des ressources pour le Ministère;
- contribuer à la mise en œuvre des processus gouvernementaux normalisés en matière de cybersécurité;
- assurer, une prise en charge rapide et concertée des événements de sécurité pour le Ministère;
- représenter le Ministère auprès de la Cellule gouvernementale de cyberdéfense;
- maintenir un registre des répondants en matière de sécurité de l'information tant au Ministère que pour les organismes rattachés au portefeuille, pour participer au Réseau d'alerte gouvernemental;

- effectuer régulièrement les vérifications de sécurité des systèmes à l'égard des menaces et des vulnérabilités et, lorsque requis, recommander les correctifs nécessaires au Ministère;
- assurer le maintien d'un registre des événements de sécurité qui relèvent du Ministère;
- assurer l'accompagnement nécessaire en sécurité opérationnelle aux organismes publics relevant du Ministère;
- exercer toute autre activité de sécurité de l'information que lui attribue le chef délégué à la sécurité de l'information.

3.2 Répondants en matière de sécurité de l'information

3.2.1 Coordonnateur organisationnel des mesures de sécurité de l'information (COMSI)

Le COMSI assume au Ministère les responsabilités suivantes :

- représenter le Ministère et participer activement au Réseau d'alerte gouvernemental, coordonné par le CERT/AQ et s'assure de mettre en œuvre les stratégies de prévention et de réaction appropriées;
- contribuer aux analyses de risques de sécurité de l'information, à identifier les menaces et les situations de vulnérabilité et à mettre en œuvre les solutions appropriées;
- identifier les MVI touchant le Ministère, en tenir informé son CSIO et les faire remonter selon les conditions définies par le processus GMVI, si nécessaire;
- s'assurer de l'élaboration, de la mise à jour et de l'application d'un plan interne de réponse aux MVI;
- collaborer étroitement avec les CSIO et ROCD en leur fournissant, notamment, le soutien technique nécessaire à l'exercice de leurs responsabilités;
- produire des bilans et des plans d'action de sécurité de l'information du Ministère;
- s'assurer 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;
- assister 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;
- mettre en œuvre les orientations internes découlant des directives gouvernementales, des politiques internes et des pratiques généralement admises à cet égard;

- contribuer à la mise en œuvre des processus officiels de sécurité de l'information du Ministère y compris la GMVI.

3.2.2 Détenteurs de l'information

Le dirigeant de toute direction générale, tout comme un cadre relevant directement d'un sous-ministre, est détenteur des ressources informationnelles, de l'information, des processus et des services d'affaires appartenant à son unité administrative, ainsi que des risques qui en découlent.

Les détenteurs de l'information (inscrits au registre d'autorité) désignés par le Ministère sont notamment chargés :

- de catégoriser l'information relevant de leur responsabilité en matière de disponibilité, d'intégrité et de confidentialité;
- d'agir comme maîtres d'œuvre des analyses de risques et de s'assurer de la prise en charge des risques résiduels;
- 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;
- 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;
- de s'assurer de l'adéquation des mesures de sécurité de l'information en vigueur par rapport aux risques encourus;
- de mettre en place les règles d'accès à l'information qui sont sous leur responsabilité, de s'assurer de leur respect et, si nécessaire, d'autoriser toute exception.

3.2.3 Gestionnaires

Les gestionnaires sont responsables de la mise en œuvre, auprès du personnel relevant de leur autorité, des dispositions de la politique de sécurité de l'information. Ils doivent principalement :

- informer leur personnel des dispositions de la politique sur la sécurité de l'information et de toute directive, standard et procédure en vigueur en matière de sécurité de l'information, ainsi que des modalités liées à leur mise en œuvre, et les sensibiliser à la nécessité de s'y conformer;
- s'assurer que les actifs informationnels mis à la disposition de leur personnel sont utilisés en conformité avec les principes généraux et les exigences de la politique de sécurité;
- s'assurer que la sécurité de l'information est prise en compte dans tout contrat de service attribué par leur unité administrative et voir à ce que tous (consultant, partenaire ou fournisseur) s'engagent à respecter les règles de sécurité de l'information du Ministère.

3.2.4 Responsable de l'architecture de la sécurité de l'information

Le responsable de l'architecture de sécurité de l'information :

- conçoit et met en œuvre l'architecture décrivant la fonction, la structure et les interrelations des composantes de sécurité de l'information;
- arrime les solutions retenues aux processus organisationnels de sécurité de l'information;
- participe à la conception et l'évaluation des composantes de sécurité de l'information des solutions d'affaires, développées ou acquises par le Ministère.

3.2.5 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 du Ministère. Plus particulièrement, il :

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

3.2.6 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 :

- 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 du Ministère;
- s'assure de la mise au rebut sécuritaire des supports de l'information;
- élabore et met en œuvre des directives, des guides et des procédures propres à son domaine d'intervention.

3.2.7 Responsable de la gestion des technologies de l'information

Le responsable de la gestion des technologies de l'information :

- contribue à l'élaboration et à la mise en œuvre de directives propres à assurer la sécurité de l'information numérique;
- met en œuvre les mesures permettant d'assurer la sécurité de l'information numérique détenue par le Ministère, dont les plans de reprise informatique en cas de sinistre;

- met en place un cadre normatif de développement assurant la prise en charge des exigences de sécurité de l'information, y compris celles reliées 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.

3.2.8 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 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 évalue, examine ou vérifie, notamment :

- 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;
- l'adéquation de l'intégration de la sécurité de l'information dans les processus d'affaires.

3.2.9 Responsable de la gestion documentaire

Le responsable de la gestion documentaire :

- collabore à la conception des systèmes informatiques, administratifs ou autres en s'assurant, qu'à toutes les étapes du cycle de vie de l'information, ces systèmes aient les qualités nécessaires à une saine gestion documentaire et à la conservation du patrimoine informationnel, à la préservation des preuves et au respect des lois;
- collabore 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.

3.2.10 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 :

- communique au CSIO les problématiques et les préoccupations de sécurité, en égard à la protection des renseignements personnels ou sensibles;
- 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.

3.2.11 Responsable du développement ou de l'acquisition des 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 reliées au respect des exigences légales de protection des renseignements personnels, à intégrer aux systèmes d'information et s'assure de leur bon fonctionnement.

3.2.12 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.

3.3 Comités

3.3.1 Comité de gouvernance de la sécurité de l'information

Le Comité de gouvernance, en tant qu'organe central de concertation ministérielle, joue un rôle essentiel dans la gouvernance de la sécurité de l'information au sein du Ministère. Plus particulièrement, il :

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

Ce comité est présidé par la sous-ministre. Il est composé du CSIO, du ROCD, du responsable de la gestion des technologies de l'information et du responsable de l'accès à l'information et de la protection des renseignements personnels. Selon les sujets traités, d'autres répondants en matière de sécurité de l'information peuvent être invités à y prendre part.

3.3.2 Comité de crise ministériel

Le Comité de crise ministériel est l'organe décisionnel principal en cas d'incident critique de sécurité de l'information. Ce groupe intervient notamment lorsque les tentatives de rétablissement des activités n'ont pas abouti ou qu'aucune mesure palliative n'a pu garantir la continuité ou la reprise rapide des services. Le comité a pour rôle, principalement de :

- autoriser la mise en œuvre de stratégies pour la gestion des incidents critiques de sécurité de l'information, en lien avec le processus GMVI.
- adopter la déclaration de sinistre proposée par le responsable de la continuité des services et approuver les budgets spéciaux associés.

- décider du déploiement ou non des plans de continuité des services.
- proposer des orientations ou actions à suivre en cas de sinistre.
- formuler des recommandations sur le délestage total ou partiel des activités du Ministère.
- communiquer avec les médias.

Le noyau permanent de ce comité est composé de divers représentants du Ministère, du CSIO, du ROCD, du COMSI, du responsable de l'accès à l'information et de la protection des renseignements personnels, du responsable de la sécurité physique, et du responsable de la continuité des services. Le comité peut inclure d'autres experts tels que des détenteurs d'information, des conseillers juridiques, technologiques, en communication avec les médias et en ressources humaines.

En complément, ce comité :

- approuve les plans d'action en réponse aux MVI;
- applique les recommandations du comité de crise gouvernemental en cas de niveau d'intervention très élevé;
- peut s'adjoindre toute personne qualifiée pour fournir un soutien adéquat dans ses prises de décision.

3.3.3 Comité tactique de la sécurité de l'information

Le Comité de sécurité de l'information est un pilier essentiel dans la structure du Ministère. Ce comité est composé du ROCD substitut, des experts en sécurité de l'information, des responsables en protection des données personnelles, des ressources humaines, de la gestion documentaire, contractuelle et de sécurité physique, de gestion intégrée des risques ainsi que d'autres représentants du Ministère au besoin.

Missions principales :

- échange de bonnes pratiques et implémentation des processus de sécurité : le comité est dédié à l'échange de bonnes pratiques en matière de sécurité de l'information;
- partage d'expertise et de savoir-faire : organiser des sessions de partage des connaissances et des compétences en sécurité de l'information parmi les membres et les unités participantes;
- mise à jour des pratiques de sécurité : veiller à ce que les dernières tendances et avancées en matière de sécurité de l'information soient intégrées dans les pratiques quotidiennes des équipes;
- présentation des processus de sécurité : superviser et accompagner les différentes équipes dans la mise en œuvre des processus de sécurité standardisés, assurant ainsi une protection cohérente à travers le Ministère.

Le comité a la capacité de s'adjoindre des experts ou conseillers qualifiés pour soutenir ses recommandations. Il peut aussi faire appel à d'autres intervenants selon les besoins. Cette structure flexible assure une gestion efficace de la sécurité de l'information et la résilience des services du Ministère, essentielle dans un contexte en perpétuelle évolution.

3.3.4 Comité d'audit

Composé de la sous-ministre, du directeur de l'audit interne et des enquêtes administratives (Responsable de l'audit interne) pour le Ministère, de la directrice adjointe de l'audit interne et de trois membres externes.

L'audit interne procure au Ministère une assurance sur le degré de maîtrise de ses opérations, lui apporte des conseils et contribue à créer de la valeur ajoutée.

Lors de mission d'assurance, l'audit interne procède à une évaluation objective en vue de formuler des conclusions à l'endroit d'activités ciblées afin que les objectifs établis soient atteints. Les missions prennent notamment la forme d'un audit de performance et peuvent concerner différents domaines d'activité du Ministère tel que les technologies de l'information.

3.4 Partenaire gouvernemental

3.4.1 Ministère de la cybersécurité et du numérique

Le Ministère est lié par une entente de service en technologies de l'information et des communications avec le MCN impliquant un partage des responsabilités, entre autres, en matière de sécurité de l'information. Via cette entente, le MCN s'engage à fournir les services dans le respect des lois, des règlements, des politiques et des directives qui lui sont applicables. Pour les actifs informationnels du Ministère qui sont sous la charge du MCN, ce dernier a comme responsabilités, dans la limite des services fournis, de:

- aviser le Ministère, dans les plus brefs délais, de tout incident de sécurité de l'information pouvant porter atteinte à la disponibilité, à l'intégrité et à la confidentialité de l'information impliquant un service offert par le MCN;
- prendre les mesures adéquates pour assurer la sécurité de ses services;
- assurer une gestion des risques de ses services, conformément aux standards et normes reconnues dans le domaine de la sécurité de l'information;
- concevoir, déployer et mettre en œuvre des contrôles permettant d'assurer une gestion optimale des évènements de sécurité de l'information survenant dans ses services ainsi que des incidents de confidentialité ;

- collaborer à toute enquête et vérification portant sur la sécurité de l'information en fournissant les traces technologiques produites par les services du MCN requises par le Ministère en respect des exigences en matière de protection des renseignements personnels ;
- assurer la gestion des communications en lien avec les incidents de sécurité de l'information affectant ses services.

4 Dispositions finales

4.1 Date d'entrée en vigueur

Le présent cadre de gestion de la sécurité de l'information est complémentaire à la Politique sur la sécurité de l'information du Ministère. Il entre en vigueur à la date de son approbation et demeure en application tant et aussi longtemps qu'il n'est pas abrogé, modifié ou remplacé par un autre cadre de gestion.

4.2 Approbation

Le présent cadre de gestion de la sécurité de l'information est approuvé par :

La sous-ministre

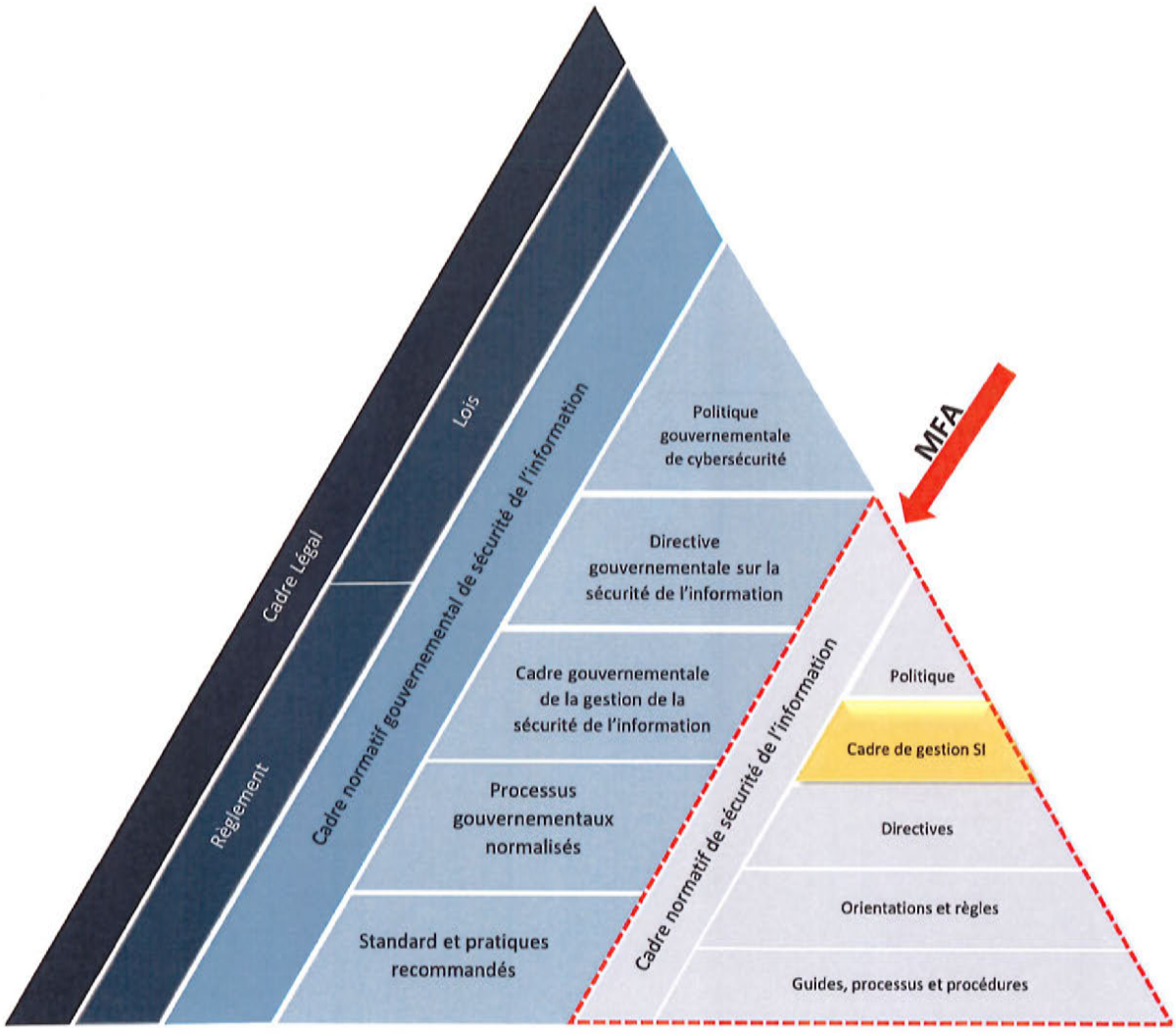
[redacted] le 26 avril 2024

Mme Julie Blackburn

Annexe 1

Représentation graphique du cadre normatif gouvernemental de sécurité de l'information

La représentation graphique suivante présente le positionnement et l'engagement du Ministère envers le cadre normatif de sécurité de l'information du gouvernement. Cette dernière, comprend le cadre de gestion de la sécurité de l'information.



Annexe 2

Cadre légal et administratif

- Charte des droits et libertés de la personne (RLRQ, chapitre C-12);
- Code civil du Québec (RLRQ);
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A- 2.1);
- Loi concernant le cadre juridique des technologies de l'information (RLRQ, chapitre C-1.1);
- Loi sur la fonction publique (RLRQ, chapitre F-3.1.1);
- Loi sur le ministère de la Cybersécurité et du Numérique (RLRQ, chapitre M-17.1.1)
- Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, chapitre G-1.03);
- Règlement sur l'éthique et la discipline dans la fonction publique (RLRQ, chapitre F-3.1.1, r. 3);
- Cadre gouvernemental de gestion de la sécurité de l'information arrêtée numéro 2022-04 du MCN en date du 26 juillet 2022 (Entrée en vigueur 10 août 2022);
- Directive gouvernementale sur la sécurité de l'information (Décret 1514-2021);
- Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1, r.2);
- Règlement sur les modalités et conditions d'application des articles 12.2 à 12.4 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (Décret 1296-2022);
- Règles sur l'assurance de l'identité numérique (Arrêté numéro 2022-05 du MCN);
- Processus de gestion des menaces, des vulnérabilités et des incidents, version 4.2 du 22-06-2022;
- Politique gouvernementale de cybersécurité (Dépôt légal – mars 2020);
- Entente de service avec le MCN (MFA_2022-000065).

Famille
Québec

Politique de gestion des risques de sécurité de l'information

Ministère de la Famille

MARS 2025

Votre gouvernement

Québec

Coordination et rédaction
Centre de la cybersécurité et services infonuagiques
Direction de la cybersécurité et des solutions de soutien
Sous ministériat au financement, aux infrastructures et à l'administration Direction générale de la transformation numérique

Historique

Révision	Date	Description du changement
0.1	2025-03-03	Version initiale
1.0	2025-04-08	Version validée

Table des matières

1. Objectif

La présente politique a pour objectif d'édicter les exigences et les lignes directrices liées à la gestion des risques de sécurité de l'information au sein du ministère de la Famille (Ministère) afin de protéger ses actifs informationnels contre les menaces internes et externes.

Définitions utiles pour lire et comprendre la présente politique

Actif informationnel : une information, un système ou un support d'information, une technologie de l'information, une installation ou un ensemble de ces éléments propriété du Ministère ou utilisé par celui-ci.

Confidentialité : propriété d'une information de n'être accessible qu'aux personnes ou aux entités désignées et autorisées.

Disponibilité : propriété d'une information d'être accessible en temps voulu et de la manière requise pour une personne autorisée.

Impact : effet d'un événement affectant les objectifs.

Intégrité : propriété associée à une information de ne subir aucune altération ou destruction sans autorisation et d'être conservée sur un support lui procurant stabilité et pérennité.

Menace : cause potentielle d'un incident lié à la sécurité de l'information qui peut entraîner des dommages pour un système ou porter préjudice à un organisme.

Risque de sécurité de l'information: est la possibilité que des menaces exploitent les vulnérabilités d'un actif informationnel ou d'un groupe d'actifs informationnels et portent ainsi un préjudice à un organisme.

Risque résiduel : risque subsistant après le traitement du risque.

Vraisemblance (Probabilité): possibilité que quelque chose se produise.

Vulnérabilité : faille dans un actif informationnel qui peut être exploitée de sorte qu'un événement ayant un impact négatif se produise (matérialisation du risque).

2. Portée

La présente politique s'applique :

- aux processus d'affaires du Ministère ;
- à tous les actifs informationnels et technologiques du Ministère autant ceux qui sont sur site que ceux qui sont externalisés et/ou hébergés chez des fournisseurs informatiques;
- au personnel du Ministère (interne et externe).

3. Lignes directrices générales

Une méthodologie de gestion des risques de sécurité de l'information doit être définie, documentée et approuvée par la haute gestion du Ministère. Cette méthodologie doit être alignée avec la politique de sécurité de l'information du Ministère et les autres standards internationaux (ex. : ISO 27005, NIST RMF, etc.).

La méthodologie de gestion des risques de sécurité de l'information doit servir pour les fins suivantes :

- définir les actifs qui seront inclus dans la gestion des risques en se basant sur leur niveau de classification et en priorisant ceux qui sont les plus critiques;
- définir les niveaux de risque en fonction de la probabilité et de l'impact sur les objectifs de sécurité : Disponibilité, Intégrité et Confidentialité (DIC);
- définir le seuil d'acceptation du risque qui détermine la tolérance au risque acceptée par le Ministère pour la paire actif/menace;
- définir les rôles et responsabilités dans le processus de gestion des risques de la sécurité de l'information.

Les recommandations émises par le Centre gouvernemental de cyberdéfense (CGCD) doivent être prises en considération dans la gestion des risques liés à la sécurité de l'information.

La gestion des risques liés à la sécurité de l'information doit être alignée avec le cadre de gestion intégrée des risques du Ministère.

Des indicateurs de performance doivent être mis en place afin de mesurer l'efficacité et l'efficience des contrôles de sécurité déployés pour protéger les actifs informationnels du Ministère.

4. Lignes directrices sur l'identification des risques

Les actifs informationnels doivent être identifiés à partir d'un inventaire tenu à jour régulièrement dans lequel chaque actif dispose d'une classification qui reflète sa valeur et sa criticité dans le système d'information du Ministère.

Les vulnérabilités et les menaces associées à chaque actif doivent être identifiées et documentées.

Les risques sur les actifs informationnels doivent être identifiés en :

- développant des scénarios de concrétisation des risques selon les vulnérabilités et menaces identifiées auparavant;
- identifiant les contrôles de sécurité déjà implantés pour mitiger les risques (risque brut);

- proposant des contrôles de sécurité administratifs, et/ou techniques et et/ou physiques pour ramener le risque à un niveau acceptable (risque résiduel).

5. Lignes directrices sur l'évaluation et la réévaluation des risques

Le Ministère doit effectuer une évaluation des risques liés à la sécurité de l'information dans les cas suivants :

- dès la phase de conception d'un projet informatique;
- avant toute modification structurante sur l'infrastructure informatique du Ministère;
- avant l'acquisition d'une solution technologique d'un fournisseur informatique;
- dans le cadre du processus d'évaluation des risques pour les actifs informationnels du Ministère.

Le Ministère doit effectuer une réévaluation des risques liés à la sécurité de l'information dans les cas suivants :

- à la suite d'un incident de sécurité qui a conduit à une compromission de la disponibilité, l'intégrité ou la confidentialité d'un ou de plusieurs actifs informationnels du Ministère;
- à la suite de conclusions d'un audit de sécurité effectué sur les actifs informationnels du Ministère et qui a soulevé des risques non identifiés ou déjà identifiés, Mais dont les mesures de mitigation mises en place par le Ministère ne sont pas jugées suffisantes pour atténuer le risque selon l'auditeur le Ministère;
- à la suite de changements majeurs dans le contexte légal et/ou réglementaire auquel est assujetti le Ministère.

6. Lignes directrices sur le traitement des risques

Le Ministère doit sélectionner l'une des options suivantes pour traiter un risque identifié :

- **Acceptation** : Le niveau du risque est acceptable, mais une surveillance doit être faite en cas d'un éventuel changement;
- **Mitigation** : Atténuer ou réduire le degré du risque en appliquant les contrôles de sécurité nécessaires pour réduire la probabilité, l'impact ou les deux, ce qui aide à contrôler le risque et à le ramener à un niveau acceptable;
- **Transfert** : Transférer le risque à un tiers qui a de meilleures capacités pour le gérer tout en étant (le Ministère) ultimement responsable de ce risque;

- **Refus** : Ne pas commencer ou arrêter l'activité porteuse du risque.

7. Lignes directrices sur la surveillance des risques

Pour surveiller les risques, le Ministère doit élaborer et tenir à jour des documents (ex. : registre des risques, plan de traitement des risques, etc.) qui doivent lui permettre de faire un suivi efficace de ces derniers. Ces documents doivent inclure à minima les informations suivantes :

- l'identifiant du risque;
- le périmètre du risque (actifs informationnels concernés);
- propriétaire du risque;
- description du risque;
- évaluation et notation du risque couvrant la probabilité et l'impact du risque et la notation globale du risque si ce dernier se concrétise;
- plan de traitement des risques couvrant l'option de traitement du risque, le propriétaire, les contrôles de mitigation et l'échéancier d'implantation de ces derniers;
- description du risque résiduel.

Un rapport de gestion des risques incluant une cartographie des risques liés à la sécurité de l'information doit être communiqué à la haute gestion du Ministère à une fréquence régulière (à minima une fois par an) ou à la suite d'un changement majeur dans le contexte de cybersécurité du Ministère.

8. Rôles et responsabilités

- **Propriétaire de la présente politique** : Chef de la sécurité de l'information organisationnelle (CSIO).
- **Revue et mise à jour de la présente politique** : Responsable opérationnel de cyberdéfense (ROCD).
- **Implémentation et mise en œuvre de la présente politique** : Responsable opérationnel de Cyberdéfense (ROCD).

9. Revue et mise à jour

- Le responsable opérationnel de cyberdéfense (**ROCD**) doit effectuer une revue de la présente politique une fois par an ou lors d'un changement majeur affectant le contexte interne ou externe du Ministère.

ANNEXE 1 : Cadre légal et normatif

Cadre légal :

- Directive gouvernementale sur la sécurité de l'information (Décret 1514-2021);
- Loi concernant le cadre juridique des technologies de l'information (LRQ, chapitre C-1.1);
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (LRQ, chapitre A-2.1);
- Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LRQ, chapitre G-1.03);
- La Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics;
- Loi concernant le cadre juridique des technologies de l'information (RLRQ, chapitre C-1.1);
- Loi sur le ministère de la Cybersécurité et du Numérique (RLRQ, chapitre M-17.1.1);
- La Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (LQ 2021, c. 25) (Loi 25).

Cadre normatif :

- Cadre de gestion des risques et des incidents à portée gouvernementale en matière de sécurité de l'information;
- Cadre gouvernemental de gestion de la sécurité de l'information arrêtée numéro 2022-04 du MCN en date du 26 juillet 2022 (Entrée en vigueur 10 août 2022);
- Processus de gestion des menaces, des vulnérabilités et des incidents, version 4.2 du 22-06-2022;
- Politique gouvernementale de cybersécurité (Dépôt légal – mars 2020);
- Les normes ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 et ISO/IEC 31000;
- La politique de sécurité de l'information du Ministère de la Famille.

Famille
Québec

Politique de confidentialité de renseignements personnels dans le cadre d'une prestation électronique de services

À L'ATTENTION DES UTILISATEURS DES SERVICES EN LIGNE

Le ministère de la Famille (Ministère) prend toutes les précautions nécessaires pour assurer la confidentialité des renseignements personnels et agit en conformité avec la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, chapitre A-2.1; ci-après « Loi sur l'accès »).

La présente politique de confidentialité décrit comment le Ministère recueille, utilise, communique, conserve et protège les renseignements personnels dans le cadre de ses services électroniques.

Elle précise les règles applicables à la collecte et à l'utilisation de renseignements personnels que le Ministère recueille par un moyen technologique ainsi que les modalités relatives au consentement d'une telle collecte ou utilisation au sens de la Loi sur l'accès.

Cette politique vous concerne si vous utilisez un service en ligne offert par le Ministère et permettant notamment de détenir un compte pour l'obtention d'une place en service de garde ou de soumettre une demande de certification à titre d'éducatrice ou éducateur en service de garde.

Collecte et utilisation des renseignements

Dans le cadre de sa prestation électronique de services, le Ministère collecte des renseignements personnels de nature confidentielle pour assurer notamment le traitement de votre dossier, l'application des lois en vigueur et l'administration de ses programmes.

Comme le prévoit la Loi sur l'accès, le Ministère recueille uniquement les données personnelles nécessaires pour permettre la mise en œuvre des services dont il est responsable. En se limitant strictement à l'essentiel, il veille à respecter votre droit à la vie privée et réduit les conséquences potentielles en cas de fuite de données.

Les renseignements personnels ainsi colligés sont conservés pour le temps nécessaire à leur utilisation ou pour plus longtems seulement lorsque cela est expressément requis par la loi. Un calendrier de conservation, approuvé par Bibliothèque et Archives nationales du Québec conformément à la *Loi sur les archives* (RLRQ, chapitre A-21.1), prévoit le moment à partir duquel un renseignement personnel peut être détruit.

Lorsque vous souhaitez bénéficier d'un service offert par le Ministère, vous avez l'obligation de fournir tous les renseignements demandés. Ne pas les fournir pourrait notamment entraîner un retard dans le traitement de votre demande ou l'impossibilité d'obtenir le service demandé. L'ensemble de ces renseignements est également nécessaire pour garantir que le service soit rendu de manière sécuritaire et conforme.

Le Ministère recueille vos renseignements personnels lorsque vous communiquez avec lui par téléphone ou à l'aide d'un moyen technologique comme un formulaire ou un questionnaire accessible en ligne, un portail numérique ou toute autre plateforme sécurisée.

Selon la prestation de services offerte, des renseignements sur votre identité et votre situation familiale ou professionnelle peuvent ainsi être recueillis, notamment : un nom, un prénom, une adresse, un numéro de téléphone, une adresse de courrier électronique, une date de naissance, certains numéros d'identification, une expérience de travail, des besoins de garde, des contraintes physiques ou comportementales, etc.

Ces renseignements permettent notamment au Ministère :

- de communiquer avec vous efficacement;
- de s'assurer de votre identité dans tous vos échanges, en vous identifiant correctement;
- d'accéder aux renseignements nécessaires au traitement de votre dossier, pour vous fournir le service demandé;
- de produire des statistiques en vue d'améliorer ses services et ses systèmes.

Vos renseignements ne seront ainsi utilisés qu'aux fins pour lesquelles ils ont été recueillis, à moins que vous ne consentiez préalablement à un autre usage ou que la Loi sur l'accès ne le permette.

Accès aux renseignements par le personnel du Ministère

Le Ministère veille à ce que seuls les membres du personnel autorisés aient accès aux renseignements personnels vous concernant. Il s'assure que ces personnes sont qualifiées pour accéder à ces renseignements et que ceux-ci sont nécessaires à l'exercice de leurs fonctions. Pour obtenir plus d'information, consultez l'inventaire des fichiers de renseignements confidentiels.

Communication des renseignements

Les renseignements personnels recueillis ne peuvent être communiqués à un autre organisme public ou être accessibles à un tiers que dans les cas prévus par la loi.

La Loi sur l'accès autorise ainsi le Ministère à communiquer des renseignements personnels à un tiers ou à un organisme public avec le consentement de la personne concernée ou encore, sans le consentement de cette dernière, dans les strictes conditions où la loi le prévoit.

Conformément à la Loi sur l'accès, le Ministère tient à jour et diffuse sur le Web des registres faisant état de ses communications de renseignements personnels, des ententes de collecte de renseignements personnels qui interviennent entre lui et d'autres organismes publics de même que les utilisations de renseignements personnels à d'autres fins que celles pour lesquelles ils ont été recueillis. Ces informations sont disponibles dans la section Registre des communications de renseignements personnels.

Conservation et destruction des renseignements

Les renseignements collectés par le Ministère sont conservés dans ses locaux et/ou hébergés sur ses serveurs. Cependant, conformément à la loi, il peut confier la conservation de certains renseignements à des tiers et ces derniers peuvent être situés, exceptionnellement, à l'extérieur du Québec. Le cas échéant, le Ministère s'assure que ces renseignements bénéficieront d'une protection équivalant à celle prévue à la Loi sur l'accès.

Conformément à la Loi sur l'accès, lorsque les fins pour lesquelles un renseignement personnel de nature confidentielle a été recueilli ou utilisé sont accomplies, le Ministère supprime celui-ci de manière sécuritaire et irrévocable, sous réserve des exigences de son calendrier de conservation et de celles de la loi.

Protection et sécurité des renseignements

Le Ministère s'assure de mettre en place des mesures de sécurité qui répondent aux plus hauts standards dans le domaine de la sécurité de l'information. Ces mesures contribuent à la protection des renseignements lors de leur collecte, de leur utilisation, de leur communication et de leur conservation jusqu'à leur destruction. Elles prévoient notamment des restrictions à l'accès, des outils technologiques de protection et de cybersécurité ainsi qu'un encadrement du personnel en matière de respect de la confidentialité.

Néanmoins, vous êtes responsable de l'information que vous acheminez au Ministère ainsi que du maintien de la confidentialité de vos données d'identification, de votre code d'accès et de votre mot de passe, s'il y a lieu.

Droits d'accès et de rectification

Le Ministère applique la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, qui vous confère les droits suivants :

- le respect de la confidentialité de vos renseignements personnels;
- le droit de demander l'accès à vos renseignements personnels et aux documents des organismes publics;

- le droit d'obtenir la rectification ou la destruction de vos renseignements personnels s'ils se révèlent incomplets, inexacts ou équivoques ou si leur collecte, leur communication ou leur conservation ne sont pas autorisées par la Loi sur l'accès.

Toute requête relative à vos droits doit faire l'objet d'une demande écrite auprès de la répondante ministérielle, qui a été désignée responsable officielle de l'accès aux documents et de la protection des renseignements personnels auprès de la Commission d'accès à l'information.

Consentement

L'utilisation de vos renseignements personnels est basée sur votre consentement. Vous pouvez à tout moment décider de le retirer, en tout ou en partie. Toutefois, un refus ou un retrait peut influer sur le traitement de votre dossier en raison de l'absence d'éléments pouvant avoir des incidences lors de l'analyse. Le cas échéant, nous vous informerons en toute transparence s'il y a des conséquences.

Par ailleurs, le Ministère ne peut recueillir les renseignements personnels de personnes mineures de moins de 14 ans sans le consentement du parent ou de la personne titulaire de l'autorité parentale.

Pour plus d'information

Si vous croyez que le Ministère n'a pas respecté sa politique de confidentialité ou si vous avez des questions relatives à la protection des renseignements personnels, vous devez vous adresser à la répondante ministérielle.

Le ministère de la Famille diffuse une Politique sur la gestion et la protection des renseignements personnels, qui traite de la gouvernance de l'information qu'il détient.

Entrée en vigueur de la politique

Cette politique est entrée en vigueur le 19 août 2025.

Directive ministérielle sur la gestion des identités et des accès logiques

MINISTÈRE DE LA FAMILLE

NOVEMBRE 2025

Votre gouvernement

Québec

Coordination et rédaction
Sous ministériat au financement, aux infrastructures et à l'administration
Direction générale de la transformation numérique
Direction de la cybersécurité et des solutions de soutien
Centre de la cybersécurité et services infonuagiques

Table des matières

1 Référentiel terminologique

Définition	Description
Accès	Possibilité d'utiliser des données ou des ressources informatiques; moyen ou voie permettant d'obtenir leur utilisation.
Actif informationnel	Information ainsi que son support, qu'il soit tangible ou intangible, permettant son traitement, sa transmission ou sa conservation aux fins d'utilisation prévue.
Accès logique	Accès à un document technologique ou capacité d'exécuter un programme ou un jeu d'instructions informatiques dans le but d'effectuer un traitement (lecture, écriture, modification ou suppression) de l'information.
Authentification	Procédure consistant à vérifier ou à valider l'identité d'un utilisateur lors d'un échange électronique, afin de contrôler son accès à un réseau, à un système informatique ou à un logiciel.
Authentifiant	Information qui, lorsqu'elle est jumelée à l'identifiant d'une personne ou d'une entité administrative ou technologique, permet de valider l'identité déclarée de cette personne ou l'identification de cette entité lors d'un accès informatique. L'authentifiant peut prendre la forme d'un mot de passe, d'un numéro d'identification personnel (NIP) ou autre, selon la technologie employée.
Compte	Droit d'accès à un ordinateur, un réseau ou un système informatique. Généralement, un compte est composé d'un identifiant et d'un mot de passe.
Compte générique	Un compte générique est un compte informatique partagé, non lié à une personne en particulier. Il est utilisé par plusieurs utilisateurs ou systèmes pour accéder à des ressources communes, comme un poste de travail partagé ou un service automatisé.
Compte à hauts privilèges	Est un compte qui a des accès et des privilèges au-delà de celui du compte standard. En règle générale ce type compte est associé aux administrateurs systèmes, administrateurs des bases de données, administrateurs de plateformes infonuagiques, etc.
Compte standard	Est un compte octroyé à un utilisateur standard avec des droits d'accès spécifiques aux fonctions qui lui sont confiées.
Contrôle d'accès	Processus par lequel des données d'authentification sont fournies par une personne ou toute autre entité, dans le but d'avoir accès à un centre ou à un système informatique. Ces données sont comparées avec des valeurs de référence touchant cette entité, ce qui permet l'autorisation ou le refus de l'accès demandés, qu'il soit physique ou logique.
Droit d'accès	Privilège accordé à un utilisateur d'avoir accès, de façon tangible ou logique, à de l'information.
Entité administrative	Ensemble organisé de personnes chargées de fournir un service administratif déterminé et capables d'interagir avec un système informatique.

Définition	Description
Entité technologique	Élément technologique (ex. : dispositif d'accès, serveur, système informatique, application informatique, objet connecté) chargé de fournir un service informatique déterminé et capable d'interagir avec d'un système informatique.
Habilitation	L'habilitation désigne l'ensemble des droits d'accès accordés à un utilisateur pour consulter ou utiliser des données, des programmes ou des systèmes. Le terme peut aussi désigner l'action d'attribuer ces privilèges, selon les besoins et les responsabilités de l'utilisateur.
Identifiant	Information associée à une personne ou à une entité. Cette information est connue de celle-ci ou est contenue sur un support informatique, dont la personne ou l'entité est détentrice et qui permet son identification.
Identité	Ensemble des données de fait et de droit qui permettent d'établir qu'une personne ou une entité est bien ce qu'elle prétend être.
Intégrité	Principe de sécurité qui assure que les données et les éléments de configuration sont modifiés uniquement par le personnel et les activités autorisés. L'intégrité considère toutes les causes possibles de modification, y compris la défaillance logicielle et matérielle, les événements liés à l'environnement et l'intervention humaine.
Référentiel des habilitations	Répertoire dans lequel sont consignés, pour chaque rôle d'affaires (fonction organisationnelle), les profils d'accès applicatifs et les profils d'accès généraux nécessaires pour accomplir les tâches associées à la fonction ainsi que les critères d'habilitation requis.
Répudiation	Répudiation fait référence à la capacité d'un utilisateur à nier avoir effectué une action ou une transaction spécifique.
Rôle	Ensemble de responsabilités, d'activités et d'autorités octroyées à une personne ou à une équipe. Le rôle est défini dans un processus.
Session	Période limitée pendant laquelle des utilisateurs authentifiés interagissent avec un système ou une application.
Utilisateur	Personne, entité administrative ou entité technologique qui font usage d'un identifiant et qui accèdent à des ressources informationnelles du Ministère.

2 Directive ministérielle sur la gestion des identités et des accès logiques

2.1 Contexte

La présente directive s'inscrit dans la mise en œuvre de la Politique de sécurité de l'information. Elle confirme la volonté du ministère de la Famille (Ministère) de renforcer l'encadrement des accès logiques afin d'assurer une gestion conforme, en tout temps, au degré de sensibilité de l'information.

La gestion des identités et des accès (GIA) et la gestion des accès logiques sont deux notions étroitement liées. Dans les pratiques de cybersécurité, elles sont souvent considérées comme complémentaires, voire équivalentes, car elles visent toutes deux à garantir que seuls les utilisateurs autorisés accèdent aux ressources numériques selon des règles précises et sécurisées.

2.2 Objectif

La présente directive a pour objectif d'établir les règles qui guideront les actions du Ministère en matière de gestion des accès logiques.

Ces règles constituent le fondement permettant de gérer et de contrôler les droits d'accès aux actifs informationnels requis pour l'accomplissement des responsabilités des utilisateurs autorisés.

2.3 Champ d'application

Cette directive s'applique à :

- L'information que détient le Ministère dans l'exercice de sa mission, que sa conservation soit assurée par lui-même ou par un tiers;
- L'information confiée au Ministère en vertu d'une entente et qui est reconnue comme devant faire l'objet d'un contrôle des droits d'accès;
- L'infrastructure technologique du Ministère;
- Toute personne physique ou morale qui, à titre d'employé, de consultant, de stagiaire, de partenaire ou de fournisseur, a un accès, sur place ou à distance, à l'information dont la sécurité est assurée par le Ministère.

3 Règles de gestion des identités et des droits d'accès logiques

3.1 Règles générales

- Un processus de gestion des accès logiques doit être documenté pour illustrer, surveiller et mettre en œuvre la création, la modification et la révocation des droits d'accès aux actifs informationnels *(un système, une application, une base de données, un programme, un service réseau, etc.)* du Ministère.

- Ce processus s'inscrit dans le cadre de la GIA, qui vise à encadrer l'ensemble du cycle de vie des identités numériques et de leurs autorisations. En intégrant la gestion des accès logiques à la GIA, le Ministère assure une approche cohérente, sécurisée et conforme à la Politique de sécurité de l'information.

- L'octroi des droits d'accès aux actifs informationnels dans un contexte d'accès à distance doit tenir compte des éléments suivants :
    - Le besoin d'affaires;
    - La criticité de l'actif informationnel;
    - Le niveau de privilège demandé par l'utilisateur;
    - Le type d'équipement utilisé par l'utilisateur dans l'accès;
    - Le lieu géographique à partir duquel l'accès est effectué.

- Des indicateurs de performance doivent être établis afin d'évaluer l'efficacité et l'efficience du processus de GIA, y compris la gestion des accès logiques. Ces indicateurs visent à mesurer la capacité du Ministère à assurer un contrôle rigoureux, sécurisé et conforme des droits d'accès aux actifs informationnels, en tenant compte du niveau de sensibilité de l'information. Ils contribuent également à l'amélioration continue des pratiques en matière de gestion des accès.

3.2 Règles liées à la gestion des identités et des authentifications

- La création de l'identité d'un utilisateur doit se faire conformément aux exigences légales et règlementaires auxquelles est assujetti le Ministère;
- L'identité numérique doit être associée à un utilisateur unique;
- Les identités et les authentifiants étant des informations confidentielles, l'utilisateur doit veiller à ne pas les divulguer à une tierce personne et à les protéger adéquatement;
- Les comptes par défaut des actifs informationnels et non nécessaires à leur fonctionnement doivent être supprimés ou minimalement désactivés;
- L'utilisation des comptes génériques pour accéder aux actifs informationnels du Ministère est proscrite;

- Dans le cas où l'utilisation des comptes génériques s'avère nécessaire pour le fonctionnement des actifs informationnels du Ministère, des contrôles compensatoires doivent être implémentés pour mitiger le risque de répudiation lié à l'utilisation de ces comptes;
- L'authentification multifactorielle est requise pour accéder aux actifs informationnels critiques du Ministère et doit être implémentée dans la mesure du possible pour les autres actifs informationnels (*par exemple, une combinaison de facteurs peut inclure : le facteur 1 — mot de passe ou NIP, et le facteur 2 — code temporaire reçu par SMS.*);
- Les contrôles d'authentification sur les actifs informationnels du Ministère doivent se faire dans la mesure du possible via un système centralisé et automatisé de contrôle des droits d'accès tel qu'Active Directory;
- Une gestion sécurisée de sessions d'utilisateurs doit être mise en place incluant :
    - Fermeture automatique de la session d'utilisateur après un délai d'inactivité déterminé;
    - Verrouillage temporaire du compte utilisateur après un nombre déterminé de connexions infructueuses.
- Les actions d'authentification effectuées par les utilisateurs sur les actifs informationnels du Ministère doivent, dans la mesure du possible, être journalisées;
- Les actions d'authentification effectuées par les comptes à haut privilège doivent être systématiquement journalisées.

3.3 Règles liées à la gestion des authentifiants

- Tout processus ou mécanisme de délivrance ou de récupération d'authentifiant doit assurer la confidentialité et l'intégrité de ce dernier. Le processus doit aussi permettre la transmission de l'authentifiant au titulaire de l'identité auquel il est associé;
- La gestion des mots de passe doit reposer sur des règles claires et accessibles à tous les détenteurs d'actifs informationnels du Ministère. Ces règles doivent couvrir la création, la complexité, la durée de validité, le renouvellement et la protection des mots de passe, afin d'assurer la sécurité des accès aux ressources numériques. Elles doivent également être diffusées et appliquées de manière cohérente dans l'ensemble des unités administratives;
- Les mots de passe par défaut des actifs informationnels doivent être modifiés avant la mise en production de ces derniers;
- Tous les actifs informationnels doivent être configurés, dans la mesure du possible, pour forcer l'utilisateur à changer son mot de passe initial/temporaire dès la première connexion.

3.4 Règles liées à la gestion des droits d'accès

- L'octroi des droits d'accès logiques doit respecter les principes suivants :
    - Le principe du privilège minimal qui exige que les utilisateurs soient octroyés uniquement les droits et autorisations nécessaires à l'exécution de leurs fonctions, pas plus;
    - Le principe du besoin d'en connaître qui exige que les utilisateurs aient des droits d'accès uniquement aux informations dont ils ont besoin dans le cadre de leurs fonctions;
    - Le principe de séparation des tâches qui exige qu'un utilisateur ne puisse pas cumuler des droits qui lui permettent de compromettre à lui seul la sécurité d'un actif informationnel ou d'effectuer des transactions frauduleuses.
- Tout octroi de droits d'accès à un actif informationnel doit être préalablement autorisé par son gestionnaire;
- L'octroi et la révocation de droits d'accès aux actifs informationnels doivent être journalisés;
- Les droits d'accès aux bases de données du Ministère par les utilisateurs doivent se faire impérativement via des applications sauf pour les administrateurs des bases de données;
- Les droits d'accès associés à une identité doivent faire l'objet d'une révision annuelle. Ce point de contrôle doit également couvrir les autorisations liées aux comptes à hauts privilèges.

3.5 Règles liées à la gestion des accès à hauts privilèges

- Les accès à hauts privilèges doivent être octroyés en fonction des tâches nécessitant des privilèges administratifs, tout en tenant compte du principe de la séparation des tâches;
- Les utilisateurs qui sont tenus et autorisés à exécuter couramment ou ponctuellement les tâches à hauts privilèges sur un actif informationnel doivent être identifiés et limités au strict minimum;
- Les comptes à hauts privilèges ne doivent pas être utilisés dans les tâches quotidiennes;
- Les comptes à hauts privilèges ne doivent ni accéder à Internet ni lire les courriels;
- L'historique des mots de passe des comptes à hauts privilèges doit être, dans la mesure du possible, activé pour suivre le nombre de mots de passe qui ont été modifiés;
- Des restrictions doivent être mises en place concernant les heures d'utilisation des comptes à hauts privilèges ainsi que les emplacements servant à l'ouverture de leurs sessions;
- Chaque utilisateur ayant un compte à hauts privilèges doit avoir un autre compte standard lui permettant d'effectuer les tâches quotidiennes;
- Des contrôles doivent être mis en place par le Ministère pour mitiger le risque lié à l'accès aux informations classifiées sensibles des bases de données aux administrateurs.

4 Rôles et responsabilités

En regard à la Politique de la sécurité de l'information, la présente directive précise les rôles et les responsabilités des intervenants en matière de gestion des droits d'accès logiques.

4.1 La Sous-ministre

- Est la première responsable de la sécurité de l'information;
- Approuve la présente directive et en assure la diffusion.

4.2 La Cheffe de la sécurité de l'information organisationnelle (CSIO)

- Élabore et mets à jour la présente directive;
- Définit et réévalue le processus de gestion des accès logiques et s'assure de sa mise en œuvre.

4.3 Le Coordonnateur organisationnel des mesures de sécurité de l'information

- Soutiens la CSIO dans l'ensemble de ses responsabilités en matière de gestion des accès logiques;
- Mets en œuvre le processus de gestion des accès logiques.

4.4 Responsable opérationnel de la cyberdéfense

- Sont en charge des validations des demandes d'accès exceptionnelles;
- Identifie les situations qui comportent des risques d'accès inappropriés aux ressources informationnelles du Ministère;
- Définis, élabore et mets en place des mécanismes pour exploiter les données nécessaires à la vérification des accès aux ressources informationnelles du Ministère;
- Utilise ces mécanismes pour détecter des cas de dérogations potentielles aux règles déontologiques (ex. : violation de la confidentialité, utilisations non autorisées des outils informatiques).

4.5 Les gestionnaires

- Contribuent à la définition des habilitations associées aux utilisateurs relevant de leur autorité et maintiennent à jour le référentiel des habilitations de leur unité administrative;

- Révisent annuellement les droits d'accès octroyés aux utilisateurs relevant de leur autorité et s'assurent d'une utilisation appropriée de ces accès;
- Doivent démontrer que les droits d'accès accordés aux utilisateurs sous leur autorité sont conformes aux exigences de la présente directive;
- Sensibilisent les utilisateurs relevant de leur autorité sur les bonnes pratiques à adopter pour respecter leurs rôles et responsabilités;
- Autorisent et justifient tout besoin d'accès à l'information des utilisateurs relevant de leur autorité.

4.6 Les détenteurs des actifs informationnels

- Définissent les profils d'accès aux actifs informationnels relevant de leur autorité et maintiennent à jour ces profils;
- Autorisent, révoquent et révisent périodiquement les accès aux actifs informationnels relevant de leur autorité;
- Approuvent les habilitations relevant de leur autorité;
- Doivent pouvoir démontrer que tous les droits d'accès octroyés aux actifs informationnels relevant de leur autorité sont conformes aux exigences de la présente directive;
- Autorisent et justifient auprès du demandeur tout besoin d'accès aux actifs informationnels relevant de leur autorité qui ne fait pas partie des habilitations approuvées et définies.

4.7 L'équipe bureautique / Délégués de sécurité

- Se conforment à la directive et au processus de gestion des identités et des accès logiques;
- Participent à l'élaboration d'un rapport détaillant les droits d'accès accordés aux utilisateurs ainsi que ceux appliqués aux actifs informationnels.

4.8 Les utilisateurs

En complément des responsabilités décrites dans la Politique ministérielle de la sécurité de l'information, ils :

- N'utilisent leurs droits d'accès que pour des tâches assignées;
- Sont responsables des accès qui leur sont octroyés et ils sont imputables auprès de leur gestionnaire de toute action exécutée en utilisant leurs identifiants et authentifiants;
- Accèdent seulement aux ressources informationnelles nécessaires à l'exercice de leurs fonctions;
- Ne conservent pas d'accès inappropriés et s'assurent qu'ils leur sont retirés au moment opportun.

5 Sanctions

Le Ministère peut prendre envers les utilisateurs qui ne respectent pas les règles énoncées dans la présente directive, des mesures administratives ou disciplinaires appropriées.

6 Personne- ressource

La gestion de la présente directive et le soutien nécessaire à son application sont assurés par la Direction de la Cybersécurité et des Solutions de Soutien.

Pour toute question relative à l'application ou à l'interprétation des dispositions de cette directive, veuillez-vous adresser à la Cheffe de la sécurité de l'information organisationnelle.

7 Documents de référence

- Loi concernant le cadre juridique des technologies de l'information (RLRQ, chapitre 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);
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1);
- Directive sur la sécurité de l'information gouvernementale (décret 7-2014, 15 janvier 2014);
- Politique ministérielle sur la gestion de la sécurité de l'information adoptée le 28 septembre 2015;
- Politique ministérielle sur l'accès à l'information et sur la protection des renseignements personnels adoptée le 31 mars 2014;
- Politique ministérielle pour l'accès aux données ressources humaines de SAGIR adoptée le 2 mars 2011;
- Politique sur la gestion des accès physiques en cours d'approbation;
- Directive ministérielle sur la gestion des risques en sécurité de l'information adoptée le 8 février 2016;
- Directive ministérielle sur la gestion des incidents de sécurité de l'information adoptée le 21 novembre 2016;
- Directive ministérielle sur l'utilisation sécuritaire des technologies de l'information en cours d'approbation;
- Cadre de gestion de la sécurité de l'information en vigueur depuis le 22 février 2016;
- Guide de gestion des accès logiques (SCT, ISBN 978-2-550-71120-9) publié en novembre 2016.
- Directive sur la gestion des identités et des droits d'accès aux actifs informationnels du ministère de la Cybersécurité et du Numérique (MCN).

Volet # 2

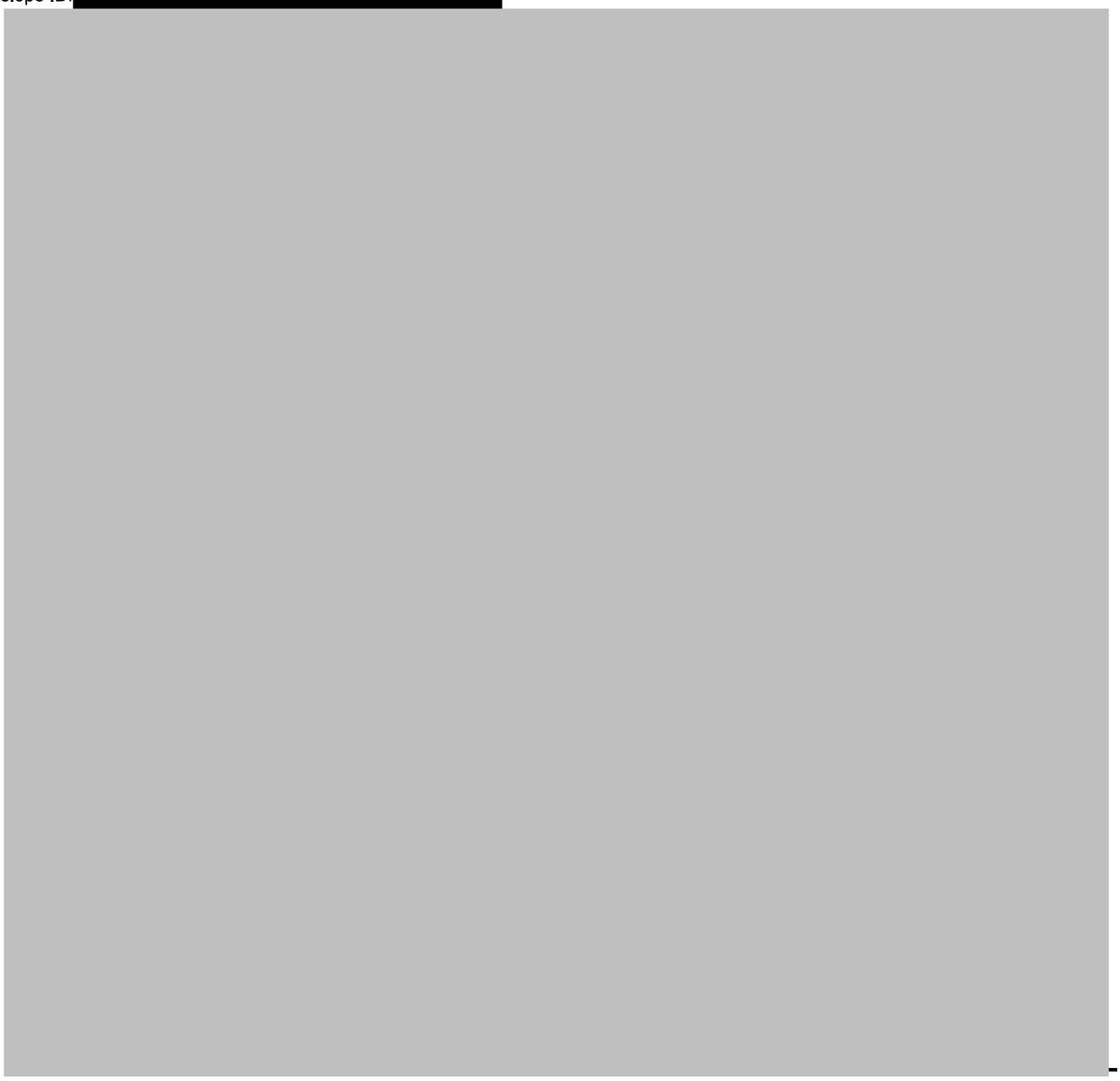
[redacted]

CS-12 LIEUX D'HÉBERGEMENT

Les lieux d'hébergement des données y incluant des renseignements personnels qui seront utilisés dans le cadre des offres sont ceux autorisés par le Courtier apparaissant au Catalogue d'offres infonuagiques.

Si en cours de contrat spécifique, le fournisseur souhaite ajouter ou modifier un ou des lieux d'hébergement, il devra en obtenir préalablement l'autorisation du Courtier comme stipulé à l'article EC-4.5.5 « Renseignements personnels hors Québec » de l'entente-cadre.

[redacted]



CS-15 ENGAGEMENT DE PROTECTION DES RENSEIGNEMENTS PERSONNELS ET CONFIDENTIELS

CS 15.1 Définitions :

Renseignement confidentiel

Tout renseignement dont l'accès est assorti d'une ou de plusieurs restrictions prévues par la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1) (Loi sur l'accès) ou par la Loi sur l'administration fiscale (RLRQ, chapitre A-6.002), notamment un renseignement personnel, un renseignement contenu dans un dossier fiscal au sens de l'article 69 de la Loi sur l'administration fiscale, un renseignement ayant des incidences sur les relations intergouvernementales, sur les négociations entre organismes publics, sur l'économie, sur l'administration de la justice et la sécurité publique, sur les décisions administratives ou politiques ou sur la vérification.

Renseignement personnel

Un renseignement est personnel lorsqu'il concerne une personne physique et permet de l'identifier. Un tel renseignement est confidentiel et ne peut être communiqué à une autre personne sauf si la personne concernée par ce renseignement y consent ou que la loi permet sa divulgation.

CS 15.2 Engagement du fournisseur

a) Les conditions contractuelles du fournisseur respectent chacune des dispositions applicables aux renseignements personnels et confidentiels ci-dessous énumérées; que ces renseignements soient communiqués au fournisseur dans le cadre de la réalisation de ce contrat ou qu'ils soient générés à l'occasion de sa réalisation. Les conditions contractuelles du fournisseur prévoient notamment que le fournisseur doit :

1) Informer son personnel des obligations stipulées aux présentes dispositions et diffuser à cet égard toute l'information pertinente.

2) 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 et sont utilisés aux fins pour lesquelles ils ont été recueillis ou que la loi autorise leur utilisation.

3) Faire signer aux membres de son personnel, préalablement à l'accès à des renseignements personnels et confidentiels, des engagements au respect de la confidentialité de ces renseignements.

4) Ne pas communiquer les renseignements personnels à qui que ce soit, sans le consentement de la personne concernée, sauf dans le cadre d'un sous-contrat ou d'un partenariat et selon les modalités prévues au paragraphe 14.

5) Soumettre à l'approbation du client le formulaire de consentement à la communication de renseignements personnels de la personne concernée.

6) Utiliser les renseignements personnels uniquement pour la réalisation du contrat.

7) Recueillir un renseignement personnel, au nom du client, 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.

8) Prendre toutes les mesures de sécurité propres à assurer la confidentialité des renseignements personnels et confidentiels à toutes les étapes de la réalisation du contrat.

9) Informer, dans les plus brefs délais, le client de tout manquement aux obligations prévues aux présentes dispositions et de tout événement pouvant risquer de porter atteinte à la sécurité ou à la confidentialité des renseignements personnels ou confidentiels.

10) Fournir, à la demande du client, toute l'information pertinente au sujet de la protection des renseignements personnels et confidentiels et donner accès à toute personne désignée par le client, à la documentation, aux systèmes et aux données relatifs au contrat afin de s'assurer du respect des présentes dispositions.

11) Se conformer aux objectifs et aux exigences de sécurité de l'information prévus à l'entente-cadre.

12) Obtenir, dans un premier temps, l'autorisation écrite du Courtier et, le cas échéant, du client, avant de communiquer ou de transférer quelle que donnée que ce soit, même à des fins techniques, hors du Québec.

13) Lorsque la réalisation du présent contrat est confiée, en tout ou en partie, à un sous-contractant ou un partenaire et qu'elle comporte la communication de renseignements personnels et confidentiels par le fournisseur au sous-contractant ou au partenaire ou la cueillette de renseignements personnels et confidentiels par le sous-contractant ou le partenaire :

    - Soumettre à l'approbation du client la liste des renseignements personnels et confidentiels communiqués au sous-contractant ou au partenaire ;

    - Conclure un contrat avec le sous-contractant ou le partenaire stipulant les mêmes obligations que celles prévues aux présentes dispositions ;

    - Exiger du sous-contractant ou du partenaire qu'il s'engage à ne conserver, à l'expiration du sous-contrat ou du partenariat, aucun document contenant un renseignement personnel ou confidentiel, quel qu'en soit le support, et à remettre au fournisseur, dans les 60 jours

suivant la fin de ce contrat, un tel document.

Dans l'éventualité où le sous-contractant est en défaut de respecter ses obligations relatives à la protection des renseignements personnels, le client se réserve le droit de résilier le contrat intervenu avec le fournisseur. Pour ce faire, le client doit adresser un avis écrit de résiliation au fournisseur. La résiliation prend effet de plein droit à la date de réception de cet avis par le fournisseur.

14) Transmettre de façon sécuritaire les renseignements personnels ou confidentiels lorsque ceux-ci sont communiqués par courriel ou Internet. Ces renseignements doivent nécessairement faire l'objet d'un chiffrement ou être protégés par un dispositif de sécurité éprouvé. Si les renseignements personnels ou confidentiels sont acheminés par télécopieur, l'émetteur du document doit s'assurer que le récepteur est habilité à le recevoir et qu'il prendra toutes les mesures nécessaires à la protection de ces renseignements. Toutefois, les parties peuvent convenir entre elles de tout autre moyen, telle la remise en mains propres, la messagerie ou la poste recommandée en indiquant toujours sur l'enveloppe la mention « personnel et confidentiel ».

b) Le fournisseur devra :

Réaliser les conditions prévues à son offre au regard de la destruction des données selon les modalités qui y sont prévues en vertu des « Conditions contractuelles du fournisseur ».

c) La fin du contrat ne dégage aucunement le fournisseur, le sous-contractant ou le partenaire de leurs obligations et engagements relatifs à la protection des renseignements personnels et confidentiels. Les principales dispositions applicables se retrouvent notamment à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, de même que dans d'autres lois prévoyant des régimes particuliers, qui peuvent être consultées à l'adresse suivante : http://legisquebec.gouv.qc.ca/fr/.

[redacted]

[redacted]

CS-17 RESPONSABILITÉ DU FOURNISSEUR

Le fournisseur est responsable de tout dommage causé par lui, ses employés, agents, représentants, partenaires ou sous-contractants dans le cours ou à l'occasion de l'exécution du présent contrat spécifique, y compris le dommage résultant d'un manquement à un engagement pris en vertu du présent contrat spécifique.

Le fournisseur s'engage à indemniser, protéger et prendre fait et cause pour le client contre tous recours, réclamation, demande, poursuite et autre procédure pris contre lui par toute personne en raison de dommages ainsi causés.

[redacted]