MINISTÈRE DES TRANSPORTS ET DE LA MOBILITÉ DURABLE

Politique de sécurité de l’information et de protection de la vie privée
Septembre 2023

GESTIONNAIRE D’ACTIFS ◆ LEADER EN MOBILITÉ

Québec

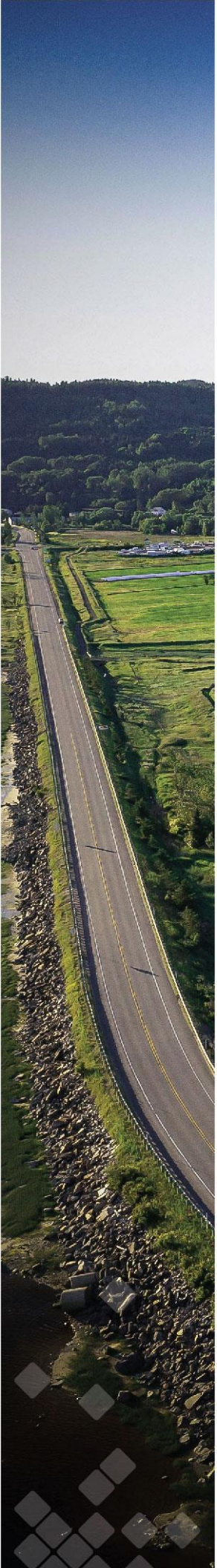

TABLE DES MATIÈRES

1. PRÉAMBULE

Dans l'accomplissement de sa mission[1], le ministère des Transports et de la Mobilité durable du Québec (MTMD), ci-après désigné « Ministère », détient de l'information sous plusieurs formes et sur plusieurs supports. Celle-ci, parfois de nature personnelle et confidentielle, possède une valeur légale, administrative et économique. Elle doit donc faire l'objet d'une utilisation appropriée et d'une protection adéquate tout au long de son cycle de vie.

Le Ministère reconnaît l'importance de protéger les citoyens, son personnel, les ressources financières qu'il gère, ses ressources matérielles ainsi que l'information et les renseignements personnels qui lui sont confiés. La mission stratégique de la gouvernance en matière de sécurité de l'information vise à réduire les risques liés aux actifs informationnels et aux comportements des usagers afin de protéger le Ministère face à la menace d'éventuelles cyberattaques et de garantir la continuité de ses services. D'où l'importance de mettre en place cette politique de sécurité de l'information et de protection de la vie privée afin d'assurer la protection des ressources informationnelles sous sa responsabilité contre tout préjudice et de pouvoir démontrer son application.

La présente politique vise à prévoir les principes directeurs qui encadrent la sécurité de l'information et la protection de la vie privée, incluant la protection des renseignements personnels au Ministère.

2. DÉFINITIONS

Les définitions des termes relatifs à la sécurité de l'information utilisés dans cette présentation sont consignées dans le document « Glossaire GSI – MTMD ». Les termes spécifiques relatifs à cette politique sont définis ci-dessous.

Actif : source de valeur pour le Ministère et qui se doit d'être gérée par l'organisation.

Actif informationnel : Une information, quel que soit son canal de communication (téléphone analogique ou numérique, télégraphe, télécopie, voix, etc.) ou son support (papier, pellicule photographique ou cinématographique, ruban magnétique, support électronique, etc.), un système ou un support d'information, une technologie de l'information, une installation ou un ensemble de ces éléments, acquis ou constitués par une organisation. Les actifs informationnels devant faire l'objet d'une analyse de préjudices/analyse de risque au Ministère sont les suivants :

1. Les applications/systèmes métiers : ce sont des applications/systèmes offrant des services à destination des clients (citoyens, entreprises, autres OP, etc.).

2. Les applications/systèmes de support métier : ils/elles concourent à l'accomplissement des activités de support (exemple: RH, gestion de projets, etc.). Ils/elles sont utilisé(e)s par les employés pour les aider dans leurs activités quotidiennes.

[1] Source : https://www.quebec.ca/gouv/ministere/transports/mission-et-mandats/

Toutes les composantes qui supportent les deux types d'actifs informationnels cités ci-haut héritent automatiquement du plus haut niveau de préjudices des systèmes auxquels elles sont liées (exemple: infrastructures technologiques, réseaux de télécommunications, technologies opérationnelles, etc.).

Cadre de gestion : document qui présente sommairement l'organisation fonctionnelle de la sécurité de l'information du Ministère et qui précise les rôles, les responsabilités et comités qui y sont impliqués.

Classification de l'information : processus permettant d'évaluer un niveau d'impact qui traduit l'importance des conséquences, sur les citoyens, le Ministère ou sur d'autres parties prenantes, d'un bris de la disponibilité, l'intégrité ou la confidentialité de l'information.

Confidentialité : propriété d'une information qui ne doit être accessible ou divulguée qu'aux personnes ou entités désignées ou autorisées.

Conformité : le fait d'être conforme aux lois, à la réglementation, aux normes ou aux politiques internes en vigueur.

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

Détenteur de l'information : titulaire d'un emploi supérieur ou cadre supérieur désigné par le Ministère comme responsable de la protection de l'information placée sous sa responsabilité. Cet employé doit appartenir à la classe d'emploi de niveau supérieur ou à une classe d'emploi de niveau cadre supérieur.

Disponibilité : propriété d'une information devant être accessible, en temps voulu et de la manière requise, par une entité autorisée.

Information : élément de connaissance concernant un phénomène et qui, pris dans un contexte déterminé, a une signification particulière.
Dans le contexte plus précis du traitement des données, une information est une donnée qui a été interprétée (ou réinterprétée).

Dans le présent contexte, il s'agit d'un actif et élément de connaissance essentiel aux activités du MTMD. Il peut être inscrit sur du papier, imprimé, stocké et transmis par voie électronique ou verbalement.

Incident de sécurité de l'information : événement qui compromet réellement ou potentiellement la confidentialité, l'intégrité ou la disponibilité d'un système d'information ou des informations que le système traite, stocke ou transmet, ou qui constitue une violation ou une menace imminente de violation des politiques de sécurité, des procédures de sécurité ou des politiques d'utilisation acceptable.

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

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

Protection de la vie privée: ensemble de mesures mises en place pour assurer le respect et la protection de la vie privée des personnes physiques contre un incident à la confidentialité, c'est-à-dire un accès non autorisé par la loi à leur renseignement personnel, à son utilisation ou à sa communication, de même que sa perte ou toute autre forme d'atteinte.

Renseignement confidentiel : information dont la divulgation non autorisée est susceptible de porter préjudice à l'individu ou à l'organisme qu'elle concerne.

Renseignement personnel : renseignement qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier.

Renseignement personnel sensible : renseignement personnel considéré comme 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 de respect de la vie privée.

Renseignement personnel à caractère public : renseignement personnel identifié par la loi comme étant à caractère public et ainsi soustrait de son régime de protection.

Risque de sécurité de l'information: risque d'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information.

Sécurité de l'information : ensemble de mesures mises en place pour assurer la protection des informations selon le niveau de confidentialité, d'intégrité et de disponibilité jugé nécessaire.

Utilisateur : toute personne, entité ou tout système informatique qui a recours aux actifs informationnels du Ministère, et à l'information qui y est consignée.

3. CADRE LÉGAL ET RÉGLEMENTAIRE

La politique de sécurité et de protection de la vie privée s'inscrit principalement dans un contexte régi par :

La Charte des droits et libertés de la personne (RLRQ, c. C-12);

Le Code civil du Québec (R.L.R.Q., c. CCQ-1991),

La Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (L.R.Q., chapitre G-1.03);

La Loi concernant le cadre juridique des technologies de l'information (RLRQ, chapitre C-1.1);

La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (R.L.R.Q., c. A -2.1), (ci-après « Loi sur l'accès »).

Le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1, r. 2);

4. 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 placée sous sa responsabilité, quel que soit son support, son moyen de communication, ou son lieu de conservation. Plus précisément, il s'agit de mettre en œuvre et de pouvoir démontrer que, tout au long du cycle de vie de l'information, sa disponibilité, son intégrité et sa confidentialité sont assurées.

En tant qu'organisme public, le Ministère doit appliquer la Loi sur l'accès. La présente politique décrit les obligations et responsabilités découlant de la Loi sur l'accès, du Règlement et du cadre administratif.

Par conséquent, le Ministère met en place cette politique dans le but d'orienter et de définir sa vision, qui sera détaillée par le cadre de gestion de la sécurité de l'information et celui relatif à la protection des renseignements personnels et de la vie privée.

5. CHAMP D'APPLICATION

La présente politique s'adresse à tout gestionnaire, détenteur et utilisateur de l'information sous la responsabilité du Ministère dans l'exercice de sa mission, peu importe que la conservation de l'information soit assurée par lui-même ou par un tiers. La politique s'applique durant tout le cycle de vie de l'information.

Cette politique vise tous les renseignements personnels détenus par le Ministère : ceux portant sur la clientèle, sur l'ensemble de son personnel, ainsi que sur des tiers. Elle s'applique aussi, quelle que soit la nature de l'information ou la forme des documents : écrite, graphique, sonore, visuelle, informatisée, etc.

6. PRINCIPES GÉNÉRAUX

En tant qu'organisme assujetti au cadre normatif en vigueur, le Ministère doit respecter les différentes obligations édictées, notamment, par cette loi, soit :

- Protéger la confidentialité des renseignements personnels détenus par le Ministère, et ce, tout au long de leur cycle de vie.
- Garantir de façon uniforme l'exercice des droits reconnus aux citoyens par la Loi sur l'accès en ce qui a trait aux renseignements personnels que le Ministère détient.
- Maintenir ou rehausser, la confiance de la population à l'égard de l'État et des services qu'il fournit et de contribuer à la réalisation de sa mission et de celle des organisations.
- Assurer la pérennité d'une information fiable.

7. PRINCIPES DIRECTEURS DE LA SÉCURITÉ DE L'INFORMATION

Une démarche notamment éthique, visant entre autres la responsabilisation collective et individuelle, soutient le processus de gestion de la sécurité de l'information.

Le Ministère assure la sécurité des ressources informationnelles et de l'information qu'il détient ou utilise conformément aux principes fondamentaux énoncés dans la politique gouvernementale en matière de sécurité de l'information en vigueur, incluant toute modification à celle-ci, et aux principes directeurs suivants :

7.1 Gouvernance et gestion de la sécurité de l'information

La gouvernance et la gestion de la sécurité de l'information reposent sur une approche ministérielle globale qui tient compte des aspects financiers, organisationnels, humains, juridiques et technologiques. Cette approche consiste en la mise en place d'un ensemble de mesures de sécurité coordonnées, cohérentes, adaptées à la mission du Ministère et supportant ses besoins d'affaires.

7.2 Évolution

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

technologiques, physiques et environnementaux, ainsi que de l'évolution des risques de sécurité de l'information afférents.

7.3 Éthique

Les processus de gouvernance et de gestion de la sécurité de l'information sont soutenus par une démarche éthique visant à assurer la régulation des conduites et la responsabilisation individuelle et organisationnelle.

7.4 Responsabilité et imputabilité

Afin d'assurer l'efficacité des mesures de sécurité de l'information, les rôles et les responsabilités, dont l'imputabilité, sont manifestement attribués à tous les niveaux du Ministère. De plus, des processus de gouvernance et de gestion de la sécurité de l'information sont en place afin de permettre une reddition de comptes adéquate.

7.5 Vérification et démontrabilité

Des vérifications sont effectuées pour évaluer l'efficacité des mesures de sécurité mises en œuvre et les résultats de ces vérifications sont validés et conservés afin de démontrer le maintien du niveau d'assurance de la protection de l'information sous la responsabilité du Ministère. Elles sont soutenues par des processus rigoureux et effectués par des personnes qualifiées dûment habilitées et ciblent aussi la détection de toute activité contrevenant aux cadres légaux, réglementaires et administratifs.

7.6 Pratiques reconnues

Les pratiques et les solutions retenues en matière de sécurité de l'information doivent être exemplaires, tenir compte des normes et des bonnes pratiques reconnues généralement utilisées à l'échelle nationale et internationale.

7.7 Transparence

L'information concernant les événements de sécurité, les pratiques et les solutions de sécurité de l'information afférentes est communiquée avec fluidité au sein du Ministère aux personnes et autorités concernées, sous réserve du droit applicable.

8. PRINCIPES DIRECTEURS DE LA PROTECTION DE LA VIE PRIVÉE

8.1 Responsabilité

Le Ministère est responsable des renseignements personnels dont il a la gestion et doit désigner un responsable de la protection des renseignements personnels chargé de veiller au respect de sa politique et de ses procédures en la matière.

8.2 Détermination des fins de la collecte des renseignements

Le Ministère doit préciser aux personnes concernées les fins pour lesquelles les renseignements personnels sont recueillis avant la collecte ou au moment de celle-ci.

8.3 Consentement

Le Ministère ne doit recueillir, utiliser, ni communiquer de renseignements personnels qu'au su et avec le consentement de la personne concernée, à moins que le consentement ne soit pas requis dans certaines circonstances particulières.

8.4 Limitation de la collecte

Le Ministère ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées et doit procéder de façon honnête et licite.

8.5 Limitation de l'utilisation, de la communication et de la conservation

Le Ministère ne doit utiliser ni communiquer de renseignements personnels à des fins autres que celles auxquelles ils ont été recueillis à moins que la personne concernée n'y consente ou que la loi ne l'exige. Le Ministère doit conserver les renseignements personnels aussi longtemps que nécessaire aux fins déterminées.

8.6 Exactitude

Le Ministère doit s'assurer que les renseignements personnels sont aussi exacts, complets et à jour que l'exigent les fins auxquelles ils sont destinés.

8.7 Mesures de sécurité

Le Ministère doit protéger les renseignements personnels au moyen de mesures de sécurité correspondant à leur degré de sensibilité et empêcher toute activité non autorisée relativement à ces renseignements.

8.8 Transparence

Le Ministère doit faire en sorte que toute personne qui lui en fait la demande par écrit puisse accéder à des renseignements précis sur sa politique et ses pratiques de protection des renseignements personnels ainsi que sur sa procédure de traitement des plaintes.

8.9 Accès à l'information

Le Ministère doit informer toute personne qui lui en fait la demande par écrit des renseignements personnels qui la concernent et que détient le Ministère, de l'usage fait de ces renseignements et du fait

qu'ils ont été communiqués à des tiers, et lui permettre de les consulter, sauf si la loi l'interdit. Par ailleurs, le Ministère doit apporter aux renseignements personnels les modifications jugées nécessaires pour les tenir à jour.

8.10 Possibilité de porter plainte à l'égard de l'inobservation des principes

Le Ministère doit fournir le moyen de porter plainte pour non-respect des principes énoncés ci-dessus auprès du responsable de la protection des renseignements personnels.

Un cadre de gestion de la protection de la vie privée doit compléter la présente Politique. Il vise à renforcer la gouvernance de la protection des renseignements personnels et de la vie privée au Ministère par la mise en place d'une structure organisationnelle en la matière, ainsi que la définition des rôles et responsabilités de chacun des intervenants concernés, et ce, à tous les niveaux.

9. SÉCURITÉ DE L'INFORMATION ET PROTECTION DES RENSEIGNEMENTS PERSONNELS

L'information détenue par le Ministère est essentielle à sa mission et doit faire l'objet d'une évaluation constante ainsi que d'une utilisation et d'une protection adéquate durant tout son cycle de vie.

Le niveau de protection accordé est établi en fonction du niveau d'impact provenant d'un risque de sécurité ou des exigences de protection de renseignements personnels, auxquels l'information est exposée.

9.1 Encadrement de la sécurité de l'information

Le Ministère met en place un comité de coordination ministérielle de la sécurité de l'information présidé par le chef de sécurité de l'information organisationnelle (CSIO) et un encadrement adéquat ainsi que des processus formels de gouvernance et de gestion de la sécurité de l'information pour s'assurer que tous les risques inacceptables, incluant ceux liés à la protection des renseignements personnels, soient systématiquement identifiés, évalués, traités et surveillés de façon continue, structurée et démontrable.

Cet encadrement qui sera précisé notamment par des directives permet aussi à l'organisation de se doter d'une vision globale, de prioriser et de concentrer les efforts et les ressources requis à la gestion et la coordination de la sécurité de l'information ministérielle.

9.2 Classification de l'information

Afin d'en définir le niveau de protection adéquat, le Ministère classifie toute information sous sa responsabilité, notamment selon son niveau de disponibilité, d'intégrité et de confidentialité. La classification doit être coordonnée et révisée et les résultats de cette dernière doivent être approuvés par le détenteur de l'information.

Le Ministère maintient un registre intégré au cadre normatif pour contenir les résultats approuvés de la classification des actifs informationnels.

9.3 Protection de l'information

Dès sa collecte ou de sa création jusqu'à sa disposition, l'information est protégée au regard du niveau de sensibilité lié à sa confidentialité, à son intégrité et à sa disponibilité.

L'information est :

a) Conservée selon la durée prévue au calendrier de conservation, lorsqu'applicable;

b) Disposée et détruite de manière sécuritaire, lorsque requis.

9.4 Protection des renseignements personnels

Tout renseignement personnel est identifié, classifié et préservé de toute divulgation, de tout accès ou de toute utilisation non autorisée ou non consentie.

Le Ministère met en place un cadre normatif et des services permettant une saine gestion des identités et des accès à l'information.

La gestion des accès prend appui sur le principe de privilège minimum et le principe de séparation de tâches.

9.5 Gestion des risques de sécurité

Le Ministère gère les risques de sécurité des ressources informationnelles sous sa responsabilité, en vue d'identifier, d'évaluer, de vérifier et de démontrer la mise en place des mesures de sécurité adéquates.

9.6 Relation avec les fournisseurs et les partenaires

Le Ministère précise les exigences de sécurité de l'information ainsi que les preuves attendues démontrant la vérification de leur mise en œuvre dans les ententes et les contrats conclus avec les fournisseurs et les autres ministères ou organismes.

9.7 Sécurité physique

Le Ministère s'assure de la mise en place des mesures de sécurité physique nécessaires à la protection de l'information sous sa responsabilité.

9.8 Sensibilisation et formation

Le Ministère encadre la sensibilisation et la formation des parties prenantes à la sécurité de l'information et à la protection de la vie privée, aux conséquences de leurs actions liées à leurs rôles, leurs responsabilités ou leurs obligations en cette matière.

9.9 Gestion des incidents

Le Ministère détecte et gère les incidents en sécurité de l'information ainsi que les incidents de confidentialité et les déclare aux autorités concernées conformément aux exigences gouvernementales en vigueur.

Le Ministère assume ses responsabilités en matière de surveillance et de gestion des menaces, vulnérabilités et incidents de sécurité, à l'égard des organismes du portefeuille Transports (STQ et CTQ) conformément aux exigences énoncées par le Centre gouvernemental de cyberdéfense (CGCD) et la Loi sur l'accès.

9.10 Conformité

Le Ministère procède à des revues régulières, à intervalles définis, et indépendants de l'approche retenue de l'organisation pour gérer et mettre en œuvre la sécurité de l'information et la protection des renseignements personnels.

9.11 Droit de regard

Le Ministère exerce un droit de regard sur tout usage de l'information sous sa responsabilité, et ce, en conformité avec le cadre légal et administratif applicable au Ministère.

10. OBLIGATIONS DES INTERVENANTS EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION ET DE PROTECTION DE LA VIE PRIVÉE

La présente politique fixe les obligations en matière de sécurité de l'information et de protection de la vie privée attribuées au sous-ministre, au chef de la sécurité de l'information organisationnelle, au responsable de l'accès à l'information et de la protection des renseignements personnels, au comité ministériel sur l'accès à l'information et la protection des renseignements personnels, aux détenteurs de l'information, aux gestionnaires et aux autres parties prenantes.

Le sous-ministre est imputable de la sécurité de l'information relevant de son autorité. Il approuve la politique et le cadre de gestion de sécurité de l'information et délègue sa mise en œuvre au chef de sécurité de l'information organisationnelle (CSIO). Le sous-ministre est le premier responsable de la protection des renseignements personnels. À ce titre, il veille au respect du cadre légal, réglementaire et administratif et s'acquitte de ses obligations telles qu'elles sont édictées dans la Loi sur l'accès.

Le chef délégué de la sécurité de l'information (CDSI) assure la coordination de la sécurité de l'information au niveau stratégique, tactique et opérationnel pour les organismes publics du portefeuille Transports Québec.

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

Le responsable de l'accès à l'information et de la protection des renseignements personnels (RAIPRP) assume de façon déléguée les fonctions dévolues au sous-ministre par la Loi sur l'accès. Le RAIPRP exerce les pouvoirs qui lui sont délégués de manière autonome.

Le comité ministériel sur l'accès à l'information et la protection des renseignements personnels soutient le sous-ministre dans l'exercice de ses responsabilités et obligations en matière d'accès à l'information et de protection des renseignements personnels.

Le responsable opérationnel de cyberdéfense (ROCD) soutient le chef délégué de sécurité de l'information (CDSI) dans la coordination et la direction de son Centre opérationnel de cyberdéfense (COCD) et représente le portefeuille Transports Québec auprès du Centre gouvernemental de cyberdéfense (CGCD).

Le détenteur de l'information doit s'assurer de la sécurité de l'information et de la protection des renseignements personnels relevant de la responsabilité de son unité administrative.

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

Toute entité qui utilise les ressources informationnelles du Ministère doit se conformer à la présente politique, aux directives et aux règles ministérielles et gouvernementales.

La description complète des rôles et des responsabilités attribués à tous les intervenants, ainsi que les structures internes de coordination et de concertation en matière de sécurité de l'information et de protection de la vie privée sont définies dans le cadre ministériel de gestion de la sécurité de l'information et le cadre ministériel de gestion de la protection de la vie privée.

11. SANCTIONS

Lorsque le Ministère ou une partie prenante contrevient à la présente politique ou aux directives en découlant, il s'expose à des mesures disciplinaires, administratives ou légales.

12. DISPOSITIONS FINALES

Le sous-ministre approuve la présente politique.

Le chef de la sécurité de l'information organisationnelle ainsi que le responsable de l'accès à l'information et de la protection des renseignements personnels sont chargés de la mise en œuvre des dispositions de la présente politique et de ses directives d'application.

La présente politique est complétée par le cadre de gestion de la sécurité de l'information et le cadre de gestion de la protection de la vie privée, chacun précisant les obligations qui en découlent.

La présente politique entre en vigueur à la date de son approbation, et par le fait même, remplace la Politique de sécurité de l'information, édition 2018.

Le Ministère est toujours à la recherche d'occasions pour améliorer ou mettre à jour ses pratiques, pour rationaliser ses activités tout en se conformant à la loi. Par conséquent, la présente politique sera révisée chaque quatre ans ou selon le besoin. La responsabilité de sa révision appartient au CSIO.

_____ _____

Sous-ministre Date

13. RÉFÉRENCES

- Loi sur les archives (RLRQ, chapitre A-21.1);
- Loi sur l'administration publique (RLRQ, chapitre A-6.01);
- Loi sur l'administration financière (RLRQ, chapitre A-6.001);
- Loi modernisant des dispositions législatives en matière de protection des renseignements personnels;
- Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics;
- Politique gouvernementale de cybersécurité, version 2019;
- Directive sur la sécurité de l'information gouvernementale, Secrétariat du Conseil du trésor, 17 septembre 2021;
- Cadre gouvernemental de gestion de la sécurité de l'information; secrétariat du Conseil du trésor, édition 2021;
- Cadre de référence gouvernementale en gestion intégrée des documents; secrétariat du Conseil du trésor, édition 2014