Direction générale adjointe

CENTRE OPÉRATIONNEL DE CYBERDÉFENSE (DGACOCD)

CYBERSÉCURITÉ

Politique provinciale de sécurité de l'information

MSSS-POL01

2022-09-19

Votre gouvernement

Ministère de la Santé et des Services sociaux

Québec

Table des matières

Préambule

L'infonuagique, l'intelligence artificielle, la mobilité, l'Internet des objets ainsi que les nouvelles technologies de stockage et de transmission de l'information sont au cœur de l'utilisation quotidienne du numérique au ministère de la Santé et des Services sociaux (MSSS) et dans les établissements et les organismes du réseau de la Santé et des Services sociaux (RSSS).

La stratégie de transformation numérique du MSSS et du RSSS permettra à terme de bonifier la prestation de services aux citoyens. Elle constitue une opportunité, mais suscite également des préoccupations majeures à considérer en lien avec la protection de l'information sensible (médicale, psychosociale, etc.) détenue par ces entités.

Dans ce contexte, le MSSS reconnaît qu'il est primordial d'assurer la disponibilité, l'intégrité et la confidentialité de cette information afin de pouvoir réaliser adéquatement les activités liées à sa mission et ainsi renforcer la confiance du citoyen à cet égard. Il concrétise cette volonté par une gouverne forte, évolutive et adaptée de la sécurité de l'information (SI) afin de contribuer activement à l'effort gouvernemental en la matière et instaurer une saine culture organisationnelle de la SI.

La présente politique constitue les assises de cette volonté. Les dispositions qui la composent sont complétées et renforcées par le cadre provincial de gestion de la sécurité de l'information ainsi que par des règles particulières et des directives sur la SI.

Objectifs

La présente politique vise :

- la prise en charge structurée et efficiente de la SI;
- le maintien de la disponibilité, de l'intégrité et de la confidentialité de l'information détenue tout au long de son cycle de vie, notamment par la réduction des risques liés à la SI;
- la concertation et la collaboration afin de favoriser l'évolution d'une saine culture de la SI;
- la cohésion des actions en SI découlant des exigences gouvernementales;
- la prise en charge optimale des événements de sécurité.

Champ d'application et portée

Cette politique s'applique aux entités suivantes :

- le MSSS;
- les organismes visés au paragraphe 5 de l'article 2 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03), ci-après appelés É/O.

Elle s'applique également à toute information détenue par ces entités, peu importe sa nature, le support sur lequel elle se trouve (enregistrement sonore ou vidéo, données électroniques ou numériques, papier, etc.) ou sa localisation (la conservation par un tiers par exemple) et ce, durant tout son cycle de vie.

Cadre légal et administratif

Cette politique fait partie du cadre de gouvernance du MSSS et s'y inscrit, sans s'y limiter, en conformité avec :

- la Loi modifiant la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LQ 2021, chapitre 22);
- la Directive gouvernementale sur la sécurité de l'information (2021);
- le Cadre gouvernemental de gestion de la sécurité de l'information.

Définitions

Pour l'application de cette politique, les termes suivants signifient :

Terme	Description
Actif informationnel	Actif au sens de la Loi sur le partage de certains renseignements de santé (LPCRS), soit, une banque d'information, un système d'information, un réseau de télécommunication, une infrastructure technologique ou un ensemble de ces éléments ainsi qu'une composante informatique d'un équipement médical spécialisé ou ultraspécialisé. Est également considéré comme un actif informationnel, tout support papier contenant de l'information.
Confidentialité	Propriété d'une information de n'être accessible, ni divulguée qu'aux personnes ou entités désignées et autorisées.
Cycle de vie de l'information	L'ensemble des étapes que franchit une information et qui vont de sa création, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction, en conformité avec le calendrier de conservation de l'organisation.
Détenteur de l'information	Un employé désigné par son organisme public, appartenant à la classe d'emploi de niveau-cadre ou à une classe d'emploi de niveau supérieur, et dont le rôle est, notamment, de s'assurer de la sécurité entourant de cette information ainsi que celle des ressources qui la sous-tendent, relevant de la responsabilité de son unité administrative.
Disponibilité	Propriété d'une information d'être accessible en temps voulu et de la manière requise par une personne autorisée.
Événement de sécurité	Toute forme d'atteinte, présente ou appréhendée, telles une cyberattaque ou une menace à la confidentialité, à l'intégrité et à la disponibilité d'une information ou d'une ressource informationnelle sous la responsabilité d'une organisation ou d'une personne agissant pour ce dernier.
Gestion intégrée des risques liés à la sécurité de l'information	Approche de gestion des risques qui repose sur une gestion globale, proactive et continue des risques liés à la sécurité de l'information à tous les niveaux hiérarchiques de l'organisation.
Intégrité	Propriété d'une information de ne subir aucune altération ou destruction de façon erronée ou sans autorisation et d'être conservée sur un support lui procurant stabilité et pérennité. L'intégrité fait référence à l'exactitude et à la complétude.
Risque lié à la sécurité de l'information	Probabilité non nulle que survienne un événement préjudiciable à la SI, plus ou moins prévisible, et qui peut affecter la réalisation des objectifs d'une organisation.

Fondements

Le ministre reconnaît que la prise en charge engagée de la SI par le MSSS et les É/O est fondamentale. Cette prise en charge contribue à l'accessibilité, pour l'ensemble de la population, à des services intégrés et de qualité qui visent l'amélioration de la santé et du bien-être des citoyens qui la composent. Elle s'appuie sur les fondements suivants :

1. Développement d'une saine culture en sécurité de l'information

Le développement d'une telle culture dans l'organisation tient compte :

- des aspects humains, organisationnels, financiers, juridiques et technologiques;
- de sa mission et de ses lignes d'affaires;
- de la pérennité de l'expertise en SI, notamment grâce à la formation continue ainsi qu'à l'attraction et à la rétention des ressources humaines;
- des activités régulières de sensibilisation et de formation en SI qui favorisent une compréhension commune et partagée par chacun des membres du personnel dans ses actions au quotidien;
- la participation active des gestionnaires au développement des compétences de leur personnel.

2. Gestion intégrée des risques liés à la sécurité de l'information

La gestion intégrée des risques liés à la SI :

- est une responsabilité organisationnelle qui représente un sous-ensemble de la gestion globale des risques de l'organisation et qui s'y intègre harmonieusement, en mode amélioration continue;
- permet à l'organisation d'identifier, d'évaluer et de traiter les risques d'atteinte à la disponibilité, à l'intégrité et à la confidentialité de l'information qu'elle détient;
- fournit une lecture des risques qui favorise la mise en place de mesures de SI proportionnelles à la valeur de l'information et aux risques encourus, réduisant ainsi ces risques de façon efficace.

3. Gestion des événements de sécurité

La gestion des événements de sécurité :

- est réalisée dans une dynamique de travail collaboratif qui implique l'ensemble des intervenants, permettant la canalisation et la mutualisation des efforts afin de corriger les situations qui exigent une intervention;
- met de l'avant une prise en charge rapide, de sa détection jusqu'à sa résolution;
- s'appuie sur un processus clair et agile afin de traiter promptement les situations qui nécessitent une escalade à un niveau supérieur. Des instances de coordination et de concertation sont en place, notamment afin d'assurer des communications fluides entre les intervenants.

Responsabilités

Fonction	Responsabilité
Chef délégué de la sécurité de l'information (CDSI)	Responsable de la SI pour le MSSS
Chef de la sécurité de l'information organisationnelle (CSIO)	Responsable de la SI pour chaque É/O
CSIO principal du MSSS	Assurer la coordination de la SI au niveau stratégique, tactique et opérationnel pour le MSSS et les É/O.
Responsable organisationnel de cyberdéfense (ROCD)	Assurer la coordination de la SI au niveau opérationnel pour le MSSS et les É/O.
CSIO d'un É/O	Assurer la responsabilité devant le CSIO principal de tout ce qui se réfère à la SI au sein de son organisation, mais également pour toute forme d'impartition chez un tiers.
Coordonnateur organisationnel des mesures de sécurité de l'information (COMSI)	Assurer la mise en place les mesures de sécurité de l'information.
➜ Les détails entourant les rôles et responsabilités du CDSI, du CSIO principal et des CSIO É/O ainsi que ceux des autres intervenants en SI, sont précisés dans le cadre provincial de gestion de la sécurité de l'information.	

Droit de regard

Le ministre exerce, en conformité avec la législation et la réglementation en vigueur, un droit de regard sur tout usage des actifs informationnels du MSSS et des É/O. Des mécanismes sont en place pour lui permettre d'exercer ce droit.

Sanctions

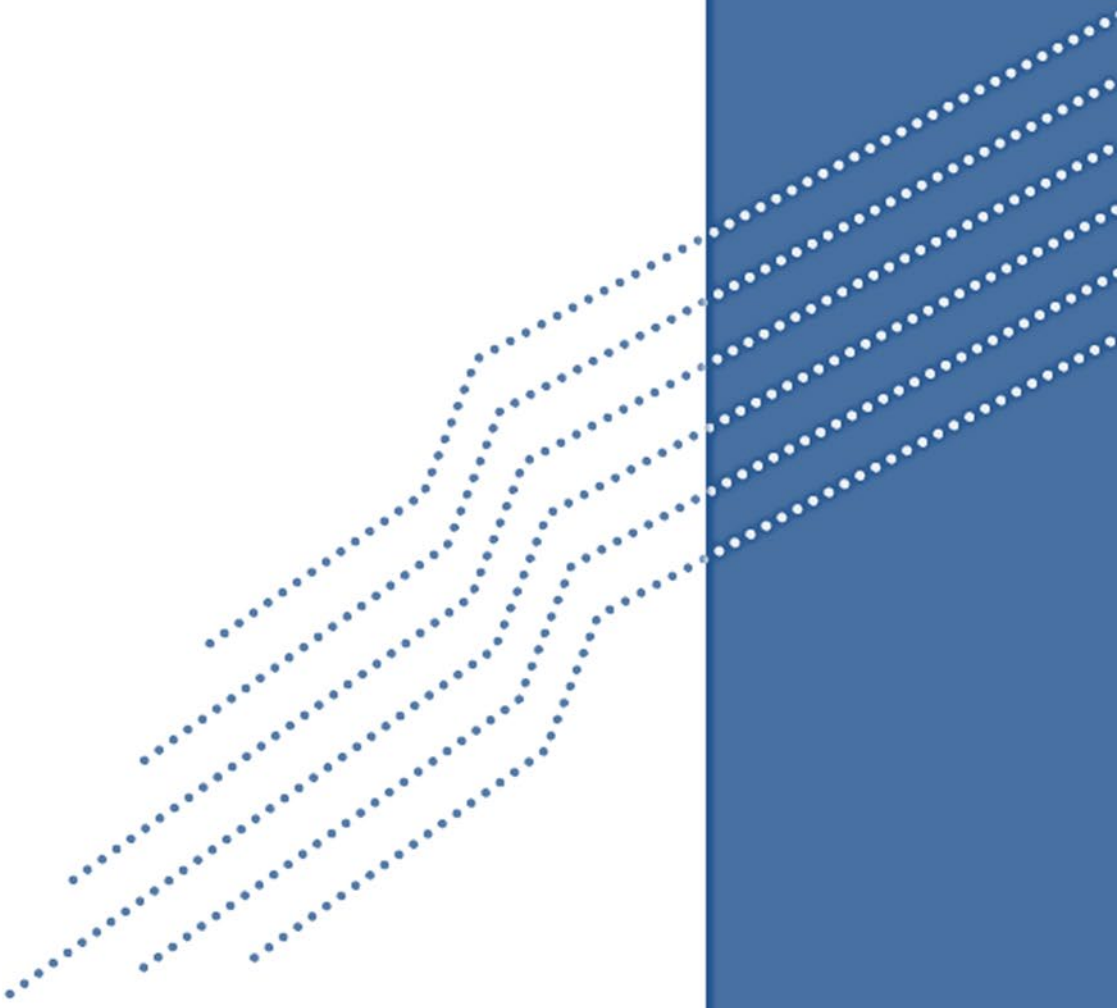
Tout manquement à la présente politique, ou à tout document qui en découle, peut faire l'objet d'une vérification effectuée par le CSIO principal du MSSS.

Entrée en vigueur et révision

Cette politique entre en vigueur à la date de son approbation. Elle doit être révisée tous les cinq ans, ou si l'une des situations suivantes se présente :

- changement organisationnel majeur;
- adoption de nouvelles orientations gouvernementales ou ministérielles.

Approuvée par le chef délégué de la sécurité de l'information (CDSI) :	Reno Bernier
Date d'approbation :	22 juillet 2022



Québec