

Direction générale adjointe

DE LA CYBERSÉCURITÉ  
ET DE L'INFONUAGIQUE (DGACI)

# CYBERSÉCURITÉ

Politique ministérielle de sécurité  
de l'information

MSSS-POL02

2023-03-01



## Table des matières

<b>Préambule</b>	<b>3</b>
<b>Objectif</b>	<b>3</b>
<b>Champ d'application et portée</b>	<b>3</b>
<b>Cadre légal et administratif</b>	<b>4</b>
<b>Définitions</b>	<b>4</b>
<b>Fondements</b>	<b>5</b>
1. Développement d'une saine culture en sécurité de l'information	5
2. Gestion intégrée des risques liés à la sécurité de l'information	5
3. Gestion des événements de sécurité	5
<b>Responsabilités</b>	<b>6</b>
<b>Droit de regard</b>	<b>6</b>
<b>Sanctions</b>	<b>6</b>
<b>Entrée en vigueur et révision</b>	<b>7</b>

---

## Préambule

---

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

La stratégie de transformation numérique dont s'est doté le MSSS 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 qu'elle détient, notamment des renseignements de nature confidentielle et stratégique.

Dans ce contexte, la sous-ministre du MSSS reconnaît qu'il est primordial d'assurer la disponibilité, l'intégrité et la confidentialité de cette information. Elle concrétise cette volonté par une gouvernance 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 de la SI au MSSS.

La présente politique constitue les assises de cette volonté. Les dispositions qui la composent sont complétées et renforcées par le cadre ministériel de gestion de la sécurité de l'information ainsi que par des directives en la matière, garantissant ainsi leur mise en œuvre auprès du personnel et des unités administratives du ministère.

---

## 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 gestion des risques liés à la SI;
- la concertation et la collaboration afin de favoriser l'évolution d'une saine culture en SI;
- la cohésion des actions en SI découlant des exigences gouvernementales et ministérielles;
- la prise en charge optimale des événements de sécurité.

---

## Champ d'application et portée

---

Cette politique s'applique à toute personne de l'organisation peu importe sa catégorie d'emploi, son statut d'employé ainsi qu'à toute personne qui, par engagement contractuel ou autrement, utilise un actif informationnel du MSSS ou y a accès.

Elle s'applique également à toute information détenue par le MSSS, 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;
- la politique provinciale sur la sécurité de l'information MSSS-POL01.

## Définitions

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

Terme	Description
<b>Actif informationnel</b>	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.
<b>Confidentialité</b>	Propriété d'une information de n'être accessible, ni divulguée qu'aux personnes ou entités désignées et autorisées.
<b>Cycle de vie de l'information</b>	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.
<b>Détenteur de l'information</b>	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.
<b>Disponibilité</b>	Propriété d'une information d'être accessible en temps voulu et de la manière requise par une personne autorisée.
<b>Événement de sécurité</b>	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.
<b>Gestion intégrée des risques liés à la sécurité de l'information</b>	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.
<b>Intégrité</b>	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.
<b>Risque lié à la sécurité de l'information</b>	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 qu'une prise en charge engagée de la SI est fondamentale. Cette prise en charge contribue ultimement à la qualité de la prestation électronique de service au citoyen et au maintien de sa confiance à l'endroit du MSSS. Elle s'appuie sur les fondements suivants :

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

Le développement d'une telle culture au MSSS 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, elle permet au MSSS de réduire ses risques de SI de façon efficace;
- permet au MSSS 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. Cette lecture des risques favorise la mise en place de mesures de SI proportionnelles à la valeur de l'information ainsi qu'aux risques encourus.

### 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 concernés, permettant la canalisation et la mutualisation des efforts afin de rectifier la situation lorsque nécessaire;
- 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)	Assurer la coordination de la SI au niveau stratégique, tactique et opérationnel pour le MSSS.
Responsable organisationnel de cyberdéfense (ROCD)	Assurer la coordination de la SI au niveau opérationnel pour le MSSS.
Coordonnateur organisationnel des mesures de sécurité de l'information (COMSI)	Assurer la mise en place des mesures de sécurité de l'information.
→ Les détails entourant les rôles et responsabilités des principaux intervenants en SI sont précisés dans le cadre ministériel de gestion de la SI qui vient compléter les dispositions de la présente politique.	

---

## 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. Des mécanismes sont en place pour lui permettre d'exercer ce droit.

---

## Sanctions

---

Lorsqu'un utilisateur contrevient ou déroge à la présente politique ou aux directives en découlant, il s'expose à des mesures disciplinaires, administratives ou légales pouvant aller jusqu'au congédiement.

---

## 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.

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.

<b>Approuvée par la sous-ministre du MSSS :</b>	Dominique Savoie
<b>Date d'approbation :</b>	1 <sup>er</sup> mars 2023

