SANTÉ QUÉBEC

Politique de sécurité de l'information

Vice-Présidence des technologies de l'information

Politique de sécurité de l’information (SI)

Adoption par le comité de gouvernance et d’éthique: 2 juin 2025

Adoption par le conseil d’administration: 12 juin 2025

Direction responsable de la politique : Direction générale de la sécurité de l’information et de la cybersécurité

Préambule

Les technologies numériques occupent et occuperont une place prépondérante dans le système québécois de santé et de services sociaux. La mobilité des personnes et des équipements utilisés[1] ainsi que l'utilisation des technologies avancées tels que l'infonuagique, l'intelligence artificielle (IA) et l'Internet des objets[2] sont, de plus en plus, intégrées dans les processus quotidiens de Santé Québec et de ses établissements. Ces innovations ainsi que les technologies déjà en place offrent des opportunités certes, mais soulèvent également d'importants défis en matière de protection des renseignements et des données ainsi que de leur utilisation. Il est donc impératif d'offrir aux citoyens un environnement résilient, performant, sécuritaire pour leurs données et services.

Pleinement consciente de ces enjeux, Santé Québec s'engage à garantir la disponibilité, l'intégrité et la confidentialité des informations détenues par ses établissements. À cette fin, la présente politique de sécurité préconise une gouvernance forte et intégrée de la sécurité de l'information, en adéquation avec la mission de Santé Québec, afin d'assurer la prévisibilité, l'accessibilité, l'efficacité et la pérennité du système québécois de santé et de services sociaux.

La présente politique traduit l'engagement ferme de la haute direction et du Conseil d'administration de Santé Québec de s'acquitter pleinement de ses obligations en sécurité de l'information et de soutenir activement les activités de protection qui en découlent. Elle établit les fondements de la stratégie provinciale de cybersécurité et intègre des dispositions concrètes alignées avec le cadre gouvernemental de sécurité de l'information ainsi que les normes et standards reconnus dans le domaine.

[1] Il s'agit notamment des tablettes, téléphone intelligent, etc.

[2] L'Internet des objets (IoT, Internet of things) caractérise les objets physiques connectés, ayant leur propre identité numérique et étant capables de communiquer les uns avec les autres par Internet ou par d'autres réseaux de connexion.

Table des matières

1. Objectifs

La présente politique vise :

- La prise en charge structurée et efficiente de la sécurité de l'information ;
- Le maintien de la disponibilité, de l'intégrité et de la confidentialité de l'information et des ressources informationnelles tout au long de leurs cycles de vie ;
- La mutualisation et la collaboration afin de favoriser l'évolution d'une saine culture de sécurité de l'information ;
- La conformité aux exigences gouvernementales et meilleures pratiques dans le domaine ;
- La gestion optimale des processus de sécurité, portant notamment sur les mesures de protection comme l'identité et les accès ou les menaces, les vulnérabilités, les incidents et les risques.

2. Champ d'application et portée

- La présente politique s'applique sans distinction à Santé Québec et aux établissements qui la composent, en vertu de la Loi sur la gouvernance du système de santé et de services sociaux.
- Elle s'applique également aux ressources informationnelles détenues par ces entités, peu importe leur nature, leur support (enregistrement sonore ou vidéo, données ou renseignements électroniques ou numériques, papier, etc.) ou leur localisation, incluant la conservation par un tiers, et ce, tout au long de leurs cycles de vie.

3. Cadre légal et administratif

Cette politique prend assise notamment sur le cadre législatif et administratif ci-dessous et y souscrit. Sans s'y limiter, il se décline ainsi :

- Loi visant à rendre plus efficace le système de santé et des services sociaux (2023, chapitre 34, aussi appelée, Loi sur la gouvernance du système de santé et de services sociaux, ci-après « LGSSSS » ;
- Loi sur les renseignements de santé et de services sociaux (RLRQ, chapitre. R -22. 1, ci-après LRSSS) ;
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.), ci-après « Loi sur l'accès ») ;

- Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, chapitre. G-1.03) ;
- Loi modifiant la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (2023, chapitre 28) ;
- Loi sur la gouvernance des sociétés d'État (RLRQ, chapitre G -1.02)
- Directive gouvernementale sur la sécurité de l'information (2021)[3];
- Cadre gouvernemental de gestion de la sécurité de l'information[4].

4. Définitions

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

Terme	Description
Actif informationnel	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 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, en conformité avec le calendrier de conservation de l'organisation.[5] Cela inclut les renseignements personnels (art. 63.1 de la loi sur l'accès).
Disponibilité	Propriété d'une information d'être accessible en temps voulu et de la manière requise par une personne autorisée.
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

[3] https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/directives/directive_securite_information2021.pdf
[4] https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/cybersecurite_numerique/Publications/CA_gestion_SI.pdf
[5] Certains actifs peuvent porter la mention « nécessité de conserver » auquel il faut tenir compte dans le cycle de vie de l'information.

Terme	Description
	lui procurant stabilité et pérennité. L'intégrité fait référence à l'exactitude et à la complétude.
Incident de confidentialité	Un accès à un renseignement personnel ou toute autre utilisation ou communication d'un renseignement personnel non autorisé par la loi, la perte d'un renseignement personnel ou toute autre atteinte à sa protection.
Incident de sécurité	Tout événement[6] ou activité qui compromet ou pourrait compromettre la confidentialité, l'intégrité ou la disponibilité des actifs informationnels d'une organisation.
Menace	Toute circonstance naturelle ou d'origine humaine qui pourrait entraîner des conséquences négatives sur un actif organisationnel.[7]
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.
Vulnérabilité	Absence ou faiblesse d'une protection d'actif qui rend une menace potentiellement plus susceptible de se produire ou susceptible de se produire plus fréquemment.[8]
Utilisateur	Toute personne physique ou morale qui utilise ou qui accède à un actif informationnel de Santé Québec ou qui utilise ses systèmes électroniques. Cela comprend notamment tout employé, gestionnaire, tout détenteur de l'information désigné par Santé Québec, ainsi que tout médecin, membre du personnel de recherche, médecin résident, stagiaire ou bénévole et toute personne qui, en vertu d'un contrat de services ou d'un mandat, dispense des services pour le compte de Santé Québec, incluant les fournisseurs, partenaires, fondations, contractuels et administrateurs.

[6] Tel que défini par la LGGRI.
[7] Centre Gouvernemental de Cyberdéfense - Processus de gestion des menaces, vulnérabilités et incidents p.19
[8] ibid. 4

5. Fondements

Afin d'assurer la résilience et la sécurité du système québécois de santé et de services sociaux, Santé Québec s'appuie sur les fondements suivants :

5.1. Structure organisationnelle et fonctionnelle agile de la sécurité de l'information

Cette structure favorise la flexibilité, la mutualisation, la collaboration et l'adaptation aux changements et met à profit l'expertise et le savoir des intervenants en sécurité du RSSS sous l'égide de Santé Québec, permettant de les mobiliser et de bénéficier de leur fort potentiel.

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

La sécurité de l'information est un domaine stratégique, transversale à l'ensemble des fonctions et processus de Santé Québec. Elle se distingue par ses enjeux et mécanismes d'action propres lui permettant de contribuer pleinement à la gestion globale des risques actuels ou émergents dans un contexte réglementaire, géopolitique et technologique en constante évolution. Elle repose notamment sur :

1. **Responsabilité organisationnelle partagée** : s'appuie sur un arrimage complémentaire entre toutes les parties prenantes, incluant la fonction de gestion intégrée des risques, et une coordination efficace à tous les niveaux de l'organisation.
2. **Détermination de l'appétit au risque et des seuils de tolérance** : en cohérence avec la mission et les objectifs stratégiques de Santé Québec, lui permettant d'innover ou de se développer.
3. **Identification et évaluation des risques** : permet à Santé Québec de maintenir à jour l'inventaire et la classification de ses actifs informationnels, d'identifier, de prioriser et de contrôler ses risques de sécurité internes et externes.
4. **Mesures d'atténuation efficaces et proportionnelles aux risques encourus** : permet la mise en œuvre de mesures de sécurité efficaces, adaptées aux risques qui leur sont associés.
5. **Amélioration continue** : par le biais du processus d'évaluation et d'optimisation des stratégies et mesures en sécurité de l'information en intégrant les leçons apprises, le suivi des indicateurs de performance afin de rehausser graduellement le niveau de maturité.
6. **Contrôle des risques liés à la chaine d'approvisionnement** : en procédant à la cartographie de la chaine d'approvisionnement, l'évaluation et la certification des fournisseurs.
7. **Registre des risques :** un dépôt d'information centralisé sur les risques identifiés permettant d'en assurer le traitement et le suivi en continu.

5.3. Gestion des identités et des accès (ci-après « GIA »)

La GIA soutient le principe de l'accès contrôlé, fondé sur le niveau d'assurance quant à l'identité du requérant, son besoin, son contexte technologique et la sensibilité des ressources informationnelles visées. Elle permet à Santé Québec de s'assurer que les bons utilisateurs, accèdent aux bonnes ressources, au bon moment et pour les bonnes raisons. À cette fin, la GIA se base sur :

1. **Directive GIA** : la directive vient notamment garantir l'équilibre entre la sécurité de l'information et l'octroi des accès et des privilèges aux utilisateurs pour l'accomplissement efficace de leurs tâches et fonctions.
2. **Processus formel de GIA** : ce processus s'intègre en cohérence avec les processus déjà en place à Santé Québec et aux établissements du RSSS.
3. **Mécanismes de contrôle des activités du personnel** : des mécanismes sont en place et leur efficacité est vérifiée périodiquement, selon les principes de base de la GIA, soit :
   - Le besoin de connaître : l'utilisateur peut uniquement accéder à l'information qu'il a besoin de connaître dans l'exercice des fonctions qu'il occupe au sein de Santé Québec.
   - Le moindre privilège : les privilèges d'accès sont octroyés de manière que l'utilisateur ne puisse accomplir que les tâches ou les activités nécessaires à l'exercice de ses fonctions.
   - La séparation des tâches : les tâches incompatibles entre elles ou conflictuelles sont séparées afin de réduire le risque d'accès ou de changements non autorisés aux actifs.
   - Le contrôle d'accès basé sur les rôles et les attributs : aucun privilège d'accès n'est directement associé à un identifiant, mais plutôt associé à un rôle.
4. **Journalisation et surveillance** : les activités des utilisateurs sont journalisées et conservées afin de permettre notamment la détection en temps réel des menaces et une réponse rapide en cas d'incident.

5.4. Gestion proactive des incidents de sécurité

Les principes fondamentaux suivant guident les actions de Santé Québec afin d'anticiper, prévenir et assurer une prise en charge rapide et efficace de tout incident de sécurité de l'information ainsi que la reprise après sinistre :

1. **Processus agile et éclairé** : l'établissement d'un tel processus permet la surveillance en continu, la détection précoce et le traitement rapide des incidents de sécurité. Il met l'emphase sur la flexibilité, l'adaptation rapide au changement et l'amélioration continue, permettant ainsi d'anticiper, de réagir rapidement et de s'ajuster aux nouvelles menaces et vulnérabilités.

2. **Dynamique de collaboration** : la gestion des incidents de sécurité est abordée de manière collaborative, engageant l'ensemble des intervenants de Santé Québec. Cette synergie permet de canaliser et de mutualiser les efforts de toutes les parties prenantes pour une prise en charge rapide et efficace.
3. **Arrimage** avec les intervenants responsables de l'accès à l'information et la protection des renseignements personnels (AIPRP) doit être réalisé afin d'assurer la cohérence et l'harmonisation des interventions de gestion des incidents de confidentialité.
4. **Coordination et concertation** : la mise en place des instances de coordination et de concertation permet d'assurer une communication fluide et transparente entre tous les intervenants, renforçant ainsi la capacité de Santé Québec à agir et réagir de manière cohérente.

5.5. Continuité des activités

La continuité des activités est un jalon important dans le plan global de continuité des services de Santé Québec. Sa mise en œuvre doit garantir la disponibilité et la fiabilité des systèmes et des informations critiques ou essentiels, en cas d'incident majeur, tel qu'une cyberattaque, une erreur humaine, une panne technique ou une catastrophe naturelle.
La continuité des activités repose notamment sur :

1. **Plan de continuité** : un plan détaillé qui définit les stratégies pour maintenir la résilience des services essentiels et critiques. Il s'appuie notamment sur le cadre de gestion intégrée des risques organisationnels, le cadre de gouvernance et gestion de l'information et les règles de gestion documentaire, les processus de gestion des crises et des incidents, le plan de reprise informatique, le plan de redondance et de contingence.
2. **Formation** : un personnel formé, quant à son rôle dans le processus de continuité des activités, garantit l'efficacité de ce processus. Des exercices de simulation en cas de sinistre doivent être réalisées régulièrement afin de le renforcer.

5.6. Certification des produits et services technologiques

Le bureau de certification de Santé Québec[9] permet d'assurer le respect des exigences concernant la sécurité, la protection des renseignements personnels, la performance ainsi que les orientations d'architecture et d'interopérabilité pour une version spécifique d'un produit ou service technologique intégré dans l'écosystème de Santé Québec.

5.7. Renforcement de la culture de sécurité de l'information

[9] Unité administrative mise en place pour répondre aux exigences légales et responsable de la coordination de l'ensemble des activités de certification.

Le facteur humain, souvent à l'origine d'attaques de grande envergure, constitue la principale vulnérabilité. Un personnel mieux formé et sensibilisé, conscient des risques liés à la sécurité de l'information, peut devenir la première ligne de défense de Santé Québec.

Le renforcement de la culture de sécurité repose sur plusieurs éléments clés dont :

1. **Aspects multidimensionnels** : cette culture tient compte des dimensions humaines, organisationnelles, financières, juridiques et technologiques.
2. **Alignement avec la mission** : en se fondant sur sa mission et ses lignes d'affaires, Santé Québec s'assure que la sécurité de l'information soit intégrée de bout en bout dans toutes ses activités.
3. **Pérennité de l'expertise** : pour garantir une expertise durable en sécurité de l'information, Santé Québec investit dans la formation de son personnel ainsi que dans des stratégies d'attraction et de rétention des talents.
4. **Sensibilisation et formation régulières** : des activités régulières de sensibilisation et de formation en SI, visant à promouvoir une compréhension partagée et commune parmi tous les membres du personnel.
5. **Participation active des gestionnaires** : les gestionnaires jouent un rôle fondamental dans le développement des compétences de leurs équipes, en favorisant une culture de la sécurité de l'information qui valorise la responsabilité collective et l'engagement de tous.

6. Responsabilités des principaux intervenants

La mise en œuvre de cette politique est une responsabilité partagée entre le Conseil d'administration, les membres de l'équipe de direction exécutive et opérationnelle[10], les établissements, et tout le personnel de Santé Québec. Ces responsabilités sont notamment définies en conformité avec les exigences de gouvernance découlant de la LGSSSS et celles liées au cadre gouvernemental de gestion de la sécurité de l'information.[11]

Fonction	Responsabilité
Provincial	
Conseil d'administration de Santé Québec et ses comités	Approuver la présente politique de sécurité; être garant de sa conformité et de son alignement avec les obligations et objectifs stratégiques; s'assurer de la performance et la

[10] Tel que défini dans le code d'éthique de Santé Québec.
[11] https://www.publicationsduquebec.gouv.qc.ca/fileadmin/gazette/pdf_encrypte/lois_reglements/2022F/78127.pdf

internes[12]	saine gestion intégrée des risques de sécurité au sein de l'organisation.
Chef délégué de la sécurité de l'information (CDSI)	Responsable de l'application de la présente politique de sécurité de l'information à Santé Québec ainsi que des dérogations ou exceptions, si requis et conformément au processus formel établi à cet effet.
Chef de la sécurité de l'information organisationnelle (CSIO)	Assurer la coordination de la sécurité de l'information sur les plans stratégique, tactique et opérationnel pour Santé Québec et son réseau.
Responsable organisationnel de cyberdéfense (ROCD)	Assurer la coordination de la cyberdéfense sur le plan opérationnel de Santé Québec.
Coordonnateur organisationnel des mesures de sécurité de l'information (COMSI)	Assurer la mise en place des mesures de sécurité de l'information de Santé Québec
Établissement	
Conseil d'administration d'établissement	Assume les responsabilités de sécurité de l'information qui lui sont attribuées ou déléguées à l'échelle de son établissement, en vertu du principe de subsidiarité et des mécanismes de délégation de pouvoirs en place à Santé Québec.
CSIO partenaire	Assurer la responsabilité auprès du CSIO de tout ce qui se réfère à la sécurité de l'information au sein de son organisation ou son secteur, mais également pour toute forme d'impartition chez un tiers.
COMSI partenaire	Assurer la responsabilité auprès du COMSI de tout ce qui se réfère à la mise en place des mesures de sécurité de l'information au sein de son organisation ou son secteur, mais également pour toute forme d'impartition chez un tiers.
➜ **Les précisions quant aux rôles et responsabilités exercés par les principaux intervenants en sécurité ainsi que ceux complémentaires, issus de domaines connexes, sont abordées dans le cadre de gouvernance et gestion de la sécurité de l'information (CGGSI)**.	

[12] Il s'agit des comités internes du CA institués en vertu la loi sur la gouvernance des sociétés d'État et de la LGSSSS notamment: le comité gouvernance et éthique, le comité d'audit, le comité de vigilance et qualité, le comité de gestion des risques. Cela inclut leurs sous-comités spécialisés.

7. Droit de regard

Santé Québec exerce, en conformité avec la législation et la réglementation en vigueur, un droit de regard sur tout usage de ses actifs informationnels. Des mécanismes sont en place pour lui permettre d'exercer ce droit et des outils peuvent être utilisés pour analyser et évaluer l'usage qui est fait de ces actifs. Santé Québec peut transmettre à toute autorité judiciaire les renseignements colligés qui la porte à croire qu'une infraction aux lois ou règlements en vigueur a été commise.

8. Sanctions

Lorsqu'un utilisateur contrevient ou déroge à la présente politique ou à tout document qui en découle, il s'expose à des mesures disciplinaires et administratives ou a toutes autres sanctions appropriées, en fonction de la gravité de son geste. Ces mesures peuvent inclure la suspension des privilèges, la réprimande, la suspension, le congédiement ou autres, et ce, conformément aux dispositions des directives, des règlements, des conventions collectives et des ententes ou des contrats en vigueur. Aussi, comme prévu à l'article 159 de la Loi sur l'accès, des pénalités en formes d'amendes s'appliquent si des manquements à ladite loi sont avérés.

9. Dispositions finales

9.1. Adoption et entrée en vigueur

La politique entre en vigueur le jour de son adoption par le conseil, le 12 juin 2025, par la résolution no CASQ-2025-06-12-09.

9.2. Prochaine révision

Le politique peut être modifiée par décision du conseil, sous recommandation du comité de transformation numérique ou du comité de gouvernance et d'éthique.