Centre intégré universitaire de santé et de services sociaux de l'Est-de-l'Île-de-Montréal

Québec

Direction générale

POLITIQUE

SÉCURITÉ DE L'INFORMATION		
Nº Politique : **POL-024**	Responsable de l'application : Chef de la sécurité de l'information organisationnelle (CSIO)	
Nº Procédure découlant : **s.o.**		
Approuvée par : **Conseil d'administration**	Date d'approbation : **2024-09-19**	Date de révision : **2027-09-19**
Destinataires : Toute personne physique ou morale qui, à titre d'employé, de consultant, de partenaire ou de fournisseur, utilise les actifs informationnels du CIUSSS-EMTL ou y a accès.		

1. CONTEXTE

Cette politique de sécurité de l'information, ci-après désignée « **politique** », est adoptée conformément à la Directive sur la sécurité gouvernementale du Secrétariat du Conseil du Trésor (SCT), décret 1514-2021 du 8 décembre 2021[1], découlant de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, R.L.R.Q., c. G-1.03*. Elle comporte notamment l'obligation pour un organisme public, d'adopter et de mettre en œuvre une politique de sécurité de l'information, de la maintenir à jour et d'en assurer l'application.
Cette directive confère aux organismes relevant du dirigeant réseau de l'information (DRI) de nouvelles obligations en matière de sécurité de l'information, de protection des renseignements personnels et de respect de la vie privée.

Le Centre intégré universitaire de santé et de services sociaux de l'Est-de-l'Île-de-Montréal (ci-après appelé «**CIUSSS-EMTL**») reconnait la nécessité d'assurer la disponibilité, l'intégrité et la confidentialité de l'information dont il a la responsabilité. Il s'engage à mettre en place une gouverne claire de la sécurité de l'information, par la définition des rôles et responsabilités à tous les niveaux du CIUSSS-EMTL et par la mise en place d'un cadre normatif de gestion, afin de répondre à ses obligations, telles que notamment décrites dans la Politique provinciale.

[1] *Directive gouvernementale sur la sécurité de l'information, décret 1514-2021 du 8 décembre 2021, Secrétariat du Conseil du Trésor*

2. CHAMP D'APPLICATION

La présente politique s'applique aux utilisateurs des actifs informationnels, c'est-à-dire à toute personne oeuvrant au sein du CIUSSS-EMTL, de quelque catégorie d'emploi et de statut d'employé que ce soit, les médecins, les médecins résidents, les dentistes, les pharmaciens, les chercheurs, le personnel de soins et services, administratif ou de soutien, les pairs aidants, les stagiaires, les bénévoles, ainsi que toute personne physique ou morale qui, par engagement contractuel ou autrement, utilise un actif informationnel du CIUSSS-EMTL ou y a accès.

L'information visée est celle que le CIUSSS-EMTL détient dans l'exercice de ses fonctions, que sa conservation soit assurée par lui-même ou par un tiers.

3. OBJECTIFS

La présente politique de sécurité de l'information a pour objectifs d'énoncer les orientations du CIUSSS-EMTL en matière de protection de l'information gouvernementale dont il a la responsabilité et d'affirmer l'engagement du CIUSSS-EMTL 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.

Cette politique sert de principale fondation et permet à l'organisme d'assurer le respect de la disponibilité, de l'intégrité et de la confidentialité (D.I.C) tout au long du cycle de vie, de tous les actifs informationnels détenus ou sous sa responsabilité.
Plus précisément, il s'agit de :

- stipuler les principes généraux et fixer les responsabilités à l'endroit des principaux intervenants en matière de sécurité de l'information ;
- structurer la prise en charge de la sécurité de l'information au sein du CIUSSS-EMTL ;
- garantir la conformité avec les orientations ministérielles et gouvernementales, notamment en matière de reddition de comptes ;
- assurer la disponibilité, l'intégrité et la confidentialité de l'information tout au long de son cycle de vie ;
- protéger les informations confidentielles détenues par le CIUSSS-EMTL.

4. DÉFINITIONS

4.1. Actif informationnel

Un actif informationnel est 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[2].

[2] *Loi concernant le partage de certains renseignements de santé,* RLRQ c P-9.0-001, art 3 (1◦).

Un actif informationnel inclut tout document constitué d'information portée par un support papier ou tout type de support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcriptibles sous l'une de ces formes ou en un autre système de symboles[3].

4.2. Autres responsables (ou autres intervenants) désignés en matière de sécurité de l'information

Il s'agit de personnes désignées pour assurer des fonctions dans des domaines connexes à la sécurité de l'information et qui ont à jouer un rôle-clé, particulièrement au regard des mesures de sécurité de l'information se rapportant à leurs domaines d'intervention respectifs.

Citons notamment à cet égard, les détenteurs de l'information ainsi que les unités responsables des ressources informationnelles, de l'accès à l'information et de la protection des renseignements personnels, de la gestion documentaire, de la sécurité physique et mesures d'urgence, ainsi que de la gestion des risques et de l'éthique.

4.3. Confidentialité de l'information

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

4.4. Cyberattaque

Ensemble coordonné d'actions malveillantes conduites par l'intermédiaire du cyberespace, qui visent à endommager, à forcer ou à détourner un réseau ou un système informatique afin de commettre un acte préjudiciable.

4.5. Cyberprotection

Ensemble des moyens, techniques ou juridiques, qui contribuent à assurer la cybersécurité.

4.6. Cyberrisque

Ensemble de risques liés à l'utilisation des technologies de l'information.

4.7. Cyberhygiène

Ensemble des règles à observer et des pratiques récurrentes qui sont associées à la sécurité d'un système d'information[4]

4.8. Cybersécurité

Capacité, pour un système en réseau, de se protéger et de résister à des événements issus du cyberespace et susceptibles de porter atteinte à la confidentialité, à l'intégrité et à la disponibilité de l'information qu'il contient.

---

[3] *Loi concernant le cadre juridique des technologies de l'information,* RLRQ c C-1., art 3.
[4] OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE. Grand dictionnaire terminologique

4.9. Cycle de vie de l'information

L'ensemble des étapes que franchit une information et qui va 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'organisme.

4.10. Disponibilité

Propriété d'une information d'être accessible en temps voulu et de la manière requise par une personne autorisée.

4.11. Gestion intégrée des risques de sécurité de l'information

Approche de gestion des risques qui repose sur une gestion globale, proactive et continue des risques de sécurité à tous les niveaux hiérarchiques de l'organisation.

4.12. Incident de sécurité ou incident de sécurité de l'information[5]

Un ou plusieurs évènements liés à la sécurité de l'information, indésirable(s) ou inattendu(s), présentant une probabilité forte de compromettre les opérations liées à l'activité de l'organisme et de menacer la sécurité de l'information (disponibilité, intégrité ou confidentialité). Un incident de sécurité de l'information peut être lié ou non à l'utilisation des technologies de l'information et des communications.

Un incident de sécurité est catégorisé selon son niveau d'impact ou de gravité.

4.13. Incident ou accident lors de la prestation des soins et services de santé[6]

- **Incident** : Action ou situation qui n'entraîne pas de conséquence sur l'état de santé ou le bien-être d'un usager, mais dont le résultat est inhabituel et qui, en d'autres occasions, pourrait entraîner des conséquences.

- **Accident** : Action ou situation où le risque se réalise et est, ou pourrait être, à l'origine de conséquences sur l'état de santé ou le bien-être de l'usager.

Un incident ou accident est catégorisé selon son niveau de gravité et ses conséquences.[7]

4.14. 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.

4.15. Mesure de sécurité de l'information Mesure de sécurité de l'information

Moyen concret assurant, partiellement ou totalement, la protection d'un actif informationnel contre un ou plusieurs risques et dont la mise en œuvre vise à amoindrir la probabilité de survenance de ces risques ou à réduire les pertes qui en résultent.

---

[5] Directive MSSS-DIR01 Déclaration des incidents de sécurité, 2015.
[6] Rapport 2014-2015 des incidents et accidents survenus lors de la prestation des soins et services de santé au Québec, MSSS, 2015.
[7] Guide sommaire GESRISK 5.0 V2014-10-21.

4.16. Principaux responsables (ou principaux intervenants) de la sécurité de l'information

Il s'agit de personnes désignées, en respect du cadre de gestion du Ministère de la Santé et des Services Sociaux (MSSS) et du Ministère de la Cybersécurité et de la Numérisation (MCN), pour assurer les fonctions de sécurité de l'information sur les plans stratégiques (dirigeant d'organisme, responsable de la sécurité de l'information ou CSIO), tactiques (CSIO, conseiller en gouvernance de la sécurité de l'information ou CGSI) et opérationnels (COMSI, coordonnateur organisation des mesures de sécurité de l'information).

4.17. Risque de sécurité de l'information

Probabilité que survienne un événement préjudiciable, dont la gravité peut être de faible à critique, qui peut affecter la réalisation des objectifs et des opérations de l'organisme.

4.18. Utilisateur

Toute personne oeuvrant au sein du CIUSSS-EMTL, de quelque catégorie d'emploi et de statut d'employé que ce soit, les médecins, les médecins résidents, les dentistes, les pharmaciens, les chercheurs, le personnel de soins et services, administratif ou de soutien, les pairs aidants, les stagiaires, les bénévoles, ainsi que toute personne physique ou morale qui, par engagement contractuel ou autrement, utilise un actif informationnel du CIUSSS-EMTL ou y a accès.

4.19. Ressources informationnelles

Les actifs informationnels ainsi que les ressources humaines, matérielles et financières directement affectées à la gestion, à l'acquisition, au développement, à l'entretien, à l'exploitation, à l'accès, à l'utilisation, à la protection, à la conservation et à l'aliénation de ces actifs.

L'ANNEXE V contient la définition d'autres termes pertinents au domaine de la sécurité de l'information.

5. ÉNONCÉ :

Le CIUSSS-EMTL reconnaît que la gouvernance de la sécurité de l'information doit être basée sur une prise en charge engagée et imputable, progressant vers la mise en avant-plan de l'amélioration continue, de la proactivité et de la reddition de comptes à tous les niveaux hiérarchiques.

Le CIUSSS-EMTL reconnait également que cette gouvernance doit favoriser une collaboration soutenue avec les principaux intervenants en sécurité de l'information et avec les autres responsables désignés, ainsi que la sensibilisation, le partage et le renforcement des connaissances.

5.1. Protection de l'information

a) Le CIUSSS-EMTL adhère aux orientations et objectifs stratégiques ministériels et gouvernementaux en matière de sécurité de l'information et s'engage à ce que les pratiques et les solutions retenues en la matière correspondent, dans la mesure du possible, à des façons de faire reconnues et généralement utilisées, tant à l'échelle nationale qu'à l'échelle internationale ;

b) Le CIUSSS-EMTL reconnaît que les actifs informationnels qu'il détient sont essentiels à ses activités courantes et, de ce fait, qu'ils doivent faire l'objet d'une évaluation constante, d'une utilisation appropriée et d'une protection adéquate ;

c) Le CIUSSS-EMTL reconnait que 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'incident, d'erreur et de malveillance auxquels ils sont exposés ;

d) Le CIUSSS-EMTL reconnait que la sécurité des actifs informationnels doit être soutenue par une démarche d'éthique visant à assurer la régulation des conduites et la responsabilisation individuelle.

5.2. Protection des renseignements confidentiels

a) Le CIUSSS-EMTL s'engage à établir et maintenir en place des mesures visant à ce que toute information confidentielle soit préservée de toute divulgation, de tout accès ou de toute utilisation non autorisée ;

b) Le CIUSSS-EMTL s'engage à assurer le respect de la vie privée des individus, notamment la confidentialité des renseignements personnels au sens de la loi[8], relatifs aux usagers et au personnel du CIUSSS-EMTL, le tout conformément aux lois et règlements en vigueur ;

Note[9] : Les renseignements personnels suivants ont un caractère public : le nom, le titre, la fonction, la classification, le traitement, les coordonnées du lieu de travail d'un membre d'un organisme public, de son conseil d'administration ou de son personnel de direction.

c) À titre indicatif, sont également considérés comme confidentiels au sens de la loi : tout renseignement dont la divulgation aurait des incidences sur les négociations entre organismes publics[10], un secret industriel[11], un renseignement industriel, financier, commercial, scientifique ou technique[12], l'administration de la justice et la sécurité publique[13], les décisions administratives ou politiques[14] et la vérification[15].

---

[8] *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels,* RLRQ c A-2.1, art 53 *[Loi sur l'accès]*
[9] *Ibid.,* art 57 (1).
[10] *Ibid.,* art 20.
[11] *Ibid.,* art 22 (1).
[12] *Ibid.,* art 22 (2) et 23.
[13] *Ibid.,* art 28 et ss.
[14] *Ibid.,* art 30 et ss.
[15] *Ibid.,* art 41 et ss.

5.3. Mise en œuvre des mesures spécifiques de sécurité des informations confidentielles

Le CIUSSS-EMTL s'engage à mettre en oeuvre les mesures de sécurité nécessaires pour la protection des informations confidentielles, incluant les renseignements personnels, notamment (mais non exclusivement) :

a) Les mesures de contrôle des accès aux renseignements confidentiels par des privilèges d'accès différents selon les catégories d'utilisateurs ;

b) Les mesures permettant de s'assurer que les actifs informationnels confidentiels ne pourront pas être utilisés et servir à d'autres fins que celles pour lesquelles ils ont été recueillis ou obtenus ;

c) Les mesures permettant d'appliquer le principe de l'attribution du « droit d'accès minimal » requis en fonction de ce qui est strictement nécessaire pour l'exécution des tâches de tout utilisateur autorisé; si le système d'information ne peut pas le permettre, des procédures de contrôles supplémentaires doivent être mises en place ;

d) Les mesures permettant de s'assurer que les ententes et contrats dont le CIUSSS-EMTL fait partie contiennent les dispositions garantissant le respect des exigences en matière de sécurité et de protection de l'information confidentielle.

5.4. Approche holistique de la sécurité de l'information

Le CIUSSS-EMTL reconnait que la gestion de la sécurité de l'information repose sur une compréhension commune et sur une approche globale qui tient compte des aspects humains, organisationnels, financiers, juridiques et technologiques. Conséquemment, le CIUSSS-EMTL met en place un ensemble de mesures coordonnées, adaptées à la nature de ses activités, supportant les besoins d'affaires et encadrées par des exigences de sécurité et des pratiques reconnues.

5.5. Journalisation

À des fins de sécurité, ou afin de respecter des exigences légales, le CIUSSS-EMTL peut mettre en place de la journalisation sur certains équipements afin de récolter les journaux d'identification et des actions prises à des fins d'audit ou d'incident.

5.6. Droits de propriété intellectuelle

Les utilisateurs doivent respecter les droits d'auteurs, les licences et autres informations en matière de propriété intellectuelle lors de l'utilisation, de la création ou de la manipulation de tout contenu, logiciel ou information propriétaire.

5.7. Gestion intégrée des risques de sécurité de l'information

a) Le CIUSSS-EMTL reconnait que la gestion intégrée des risques de sécurité de l'information est une responsabilité organisationnelle qui requiert la planification et la mise en place d'un système de gestion. Cette gestion des risques doit intégrer progressivement le principe d'amélioration continue et l'identification, l'analyse et le traitement des risques de sécurité à tous les niveaux hiérarchiques du CIUSSS-EMTL ;

b) Le CIUSSS-EMTL identifie et évalue, sur une base régulière, et dans le cadre de projets d'informatisation ou d'organisation de processus opérationnels, les risques d'atteinte à la disponibilité, l'intégrité et la confidentialité de l'information, pouvant affecter la réalisation de sa mission; il met en place des mesures permettant de réduire ces risques ;

c) Le CIUSSS-EMTL s'engage à mettre en place un système de réévaluation périodique de son niveau de sécurité par des audits qui assurent une vigie constante de la gestion de la sécurité de l'information ;

d) Le CIUSSS-EMTL met en oeuvre des processus de gestion de la sécurité de l'information qui assurent le respect des exigences de sécurité de l'information, par des pratiques recommandées en matière de sécurité de l'information ;

e) Le CIUSSS-EMTL s'engage à s'assurer que tout manquement à la sécurité de l'information fasse l'objet d'une vérification et d'une résolution par la (les) direction(s) concernée(s) et soit inscrit au registre des incidents accidents et au registre des incidents de sécurité de l'information par l'équipe de Cybersécurité, selon les procédures dans l'outil Octopus ;

f) Selon le niveau de gravité d'un manquement à la sécurité de l'information, le CSIO du CIUSSS-EMTL doit être avisé de la situation afin de s'assurer de la prise en charge des incidents de sécurité de l'information non résolus et de la reddition de comptes à la direction du CIUSSS-EMTL, au MSSS et au MCN.

5.8. Sensibilisation et formation

Le CIUSSS-EMTL reconnait que la sensibilisation et la formation du personnel en sécurité de l'information sont indispensables à l'implantation d'une culture de sécurité à l'échelle de l'organisation :

a) Le CIUSSS-EMTL s'engage, sur une base régulière, à sensibiliser et à offrir de la formation aux utilisateurs concernant la sécurité de l'information, les conséquences d'une atteinte à la sécurité, ainsi que leur rôle et leurs obligations en tant qu'utilisateurs des actifs informationnels du CIUSSS-EMTL ;

b) Le CIUSSS-EMTL s'engage à ce que les principaux intervenants en sécurité de l'information, les autres responsables désignés et les directions reçoivent une formation et le soutien nécessaire, afin de s'assurer qu'ils maîtrisent les concepts de base en sécurité de l'information et prennent des décisions éclairées.

5.9. Droit de regard

a) Le CIUSSS-EMTL exerce, en conformité avec les lois et règlements en vigueur, un droit de regard sur tout usage de ses actifs informationnels ;

b) En conséquence, les directions du CIUSSS-EMTL se réservent un droit de vérifier et valider l'utilisation faite de ses actifs informationnels, notamment par la revue des données de journalisation des accès des utilisateurs, à l'aide des outils mis à leur disposition par la Direction des ressources technologiques, et par des audits généraux.

5.10. Obligations principales en matière de sécurité de l'information

La présente politique fixe les obligations en matière de sécurité de l'information attribuées notamment au dirigeant, au CSIO, au comité de sécurité de l'information, aux détenteurs de l'information, aux directions et aux utilisateurs :

a) **Le CIUSSS-EMTL** est responsable devant le MSSS du respect de la présente politique et conserve ses responsabilités dans toute forme d'impartition. À ce titre, il précise ses exigences en matière de sécurité de l'information dans toute entente ou contrat signé avec un partenaire interne ou externe, ou un fournisseur ;

b) **Le dirigeant du CIUSSS-EMTL** : le président-directeur général, qui agit à titre de dirigeant du CIUSSS-EMTL, est le premier responsable de la sécurité de l'information relevant de son autorité. À ce titre, il prend les moyens nécessaires à la mise en oeuvre et à la gestion de la sécurité de l'information du CIUSSS-EMTL ;

c) **La direction générale adjointe-FSAP** : elle oriente les actions, approuve les décisions et fait des recommandations en matière de sécurité de l'information. Elle appuie le dirigeant du CIUSSS-EMTL par ses travaux, reçoit et valide toute question, information et document stratégique ou tactique qui émanent du CSIO, avant qu'ils ne soient déposés au président-directeur général ou au comité de vérification du conseil d'administration

d) **Chef de la sécurité de l'information organisationnelle (CSIO**) : il assiste le dirigeant du CIUSSS-EMTL dans la détermination des orientations stratégiques et des priorités d'intervention. Le CSIO, délégué par le dirigeant du CIUSSS-EMTL, est responsable de l'application de la Politique de sécurité de l'information (POL-024) ;

e) **Le comité de sécurité de l'information** : présidé par le CSIO, ce comité est l'instance de concertation en matière de sécurité de l'information. Il permet d'appuyer le dirigeant du CIUSSS-EMTL dans le respect de ses obligations concernant la sécurité de l'information ;

f) **Les détenteurs de l'information** : employés désignés par le dirigeant du CIUSSS-EMTL ou son délégué, appartenant à la classe d'emploi de niveau cadre 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 leurs unités administratives ;

g) **Les directions** : elles sont chargées de la mise en oeuvre des dispositions de la présente politique auprès de toute personne oeuvrant au CIUSSS-EMTL et relevant de leur autorité ;

h) **Les utilisateurs** : ils doivent se conformer à la présente politique, aux directives et aux règles qui leur sont applicables, et signer le *Formulaire d'engagement à la confidentialité et au respect de l'éthique*, dont une copie est jointe à la présente politique (ANNEXE I).

5.11. Obligations particulières des utilisateurs

Tout utilisateur étant autorisé à avoir accès à des actifs informationnels du CIUSSS-EMTL assume des responsabilités particulières en matière de sécurité de l'information, notamment en termes de protection de l'information, et répond de ses actions auprès du responsable désigné. Tout utilisateur a donc l'obligation de protéger les actifs informationnels mis à sa disposition par le CIUSSS-EMTL et à cette fin, il doit :

a) prendre connaissance de la présente politique, des directives, codes d'éthique, guides, mesures, et procédures en découlant, y adhérer et prendre l'engagement de s'y conformer, et signer le *Formulaire d'engagement à la confidentialité et au respect de l'éthique*, dont une copie est jointe à la présente politique (ANNEXE I) ;

b) utiliser, dans le cadre 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 ;

c) 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 ou les désactiver ;

d) se conformer aux exigences légales portant sur l'utilisation des produits à l'égard desquels des droits de propriété intellectuelle pourraient exister ;

e) signaler immédiatement selon la politique de gestion des incidents de sécurité de l'information (POL-061), tout acte ou situation 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 CIUSSS-EMTL :

   1. en avisant son supérieur de l'événement ou, si le contexte ne le permet pas, en avisant alors le CSIO du CIUSSS-EMTL ;

   2. ou dans le cas d'un contractant externe, en avisant son employeur ou le responsable du CIUSSS-EMTL auquel il se rapporte ;

   3. et obligatoirement, en faisant une déclaration d'incident ou d'accident à l'aide du formulaire AH-223, lorsque l'événement est survenu lors d'une prestation de soins ou de services aux usagers.

f) au moment de son départ du CIUSSS-EMTL, remettre les différents moyens d'identification et d'accès, les actifs informationnels, ainsi que tout l'équipement mis à sa disposition dans le cadre de l'exercice de ses fonctions.

5.12. SANCTIONS

Lorsqu'un utilisateur contrevient ou déroge à la présente politique ou aux directives, codes d'éthique, guides, mesures et procédures en découlant, il s'expose notamment 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, la fin de contrat ou autre, et ce, conformément aux dispositions des conventions collectives, des ententes ou des contrats.

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

5.13. REDDITION DE COMPTES

Le CIUSSS-EMTL met en place des mécanismes pour permettre de démontrer à sa direction, à son conseil d'administration et au MSSS, une prise en charge maîtrisée de la sécurité de l'information au niveau organisationnel, conformément à la Politique provinciale et à la Directive sur la sécurité de l'information gouvernementale.

6. RÔLES ET RESPONSABILITÉS

6.1. Le conseil d'administration du CIUSSS-EMTL

Il adopte la politique établie par le CIUSSS-EMTL en matière de sécurité de l'information et ses mises à jour, et s'assure de leur application.

6.2. Le comité de direction

Il recommande au conseil d'administration l'adoption de la politique de sécurité de l'information établie par le CIUSSS-EMTL et ses mises à jour, et en suit l'application.

6.3. Chef de Sécurité de l'Information Organisationnelle (CSIO)

- Diffuser la politique et s'assurer de sa mise en application au sein de son organisme principalement auprès des utilisateurs ;
- Maintenir à jour les politiques et directives de sécurité ;
- Développer et mettre à jour la documentation connexe ;
- Diffuser l'information ;
- Enquêter sur tout incident de sécurité susceptible de menacer la confidentialité, l'accessibilité ou l'intégrité des données et actifs informationnels ;
- Évaluer et gérer les risques de sécurité ;
- S'assurer de la conformité aux normes et aux réglementations ;
- Effectuer le suivi des incidents de sécurité.

6.4. Coordonnateur Organisation des Mesures de Sécurité de l'Information (OMSI)

- Contribuer à la mise en place des activités opérationnelles de sécurité de l'information, plus précisément, la planification, le déploiement, l'exécution, la surveillance, les enquêtes et l'amélioration des processus de sécurité nécessaires à la gestion opérationnelle de la sécurité au CIUSSS-EMTL ;
- Contribuer aux analyses de risques de sécurité de l'information, identifier les menaces et les situations de vulnérabilité et mettre en œuvre les solutions appropriées ;
- Fournir l'expertise nécessaire à l'exercice des responsabilités de son CSIO et au support du service ;
- S'assurer de la production des rapports des processus de sécurité de l'information (incidents, vulnérabilités).

6.5. Les directions des ressources humaines, des communications, de l'enseignement, de la recherche et de l'innovation, de l'approvisionnement et logistique

Elles sont responsables, notamment, d'informer toute nouvelle personne oeuvrant au sein du CIUSSS-EMTL ou tout nouveau fournisseur ou partenaire du CIUSSS-EMTL, sous leur responsabilité, dès son accueil ou le début de son mandat, de ses obligations découlant de la politique en vigueur en matière de sécurité de l'information.

6.6. Utilisateurs

- Respecter la présente politique ;
- Être responsables de l'utilisation qu'ils font des technologies de l'information ;
- Informer leur supérieur immédiat de toute violation des mesures de sécurité dont ils pourraient être témoins ou de toutes anomalies décelées pouvant nuire à la protection des actifs informationnels dans le cadre de leur travail ;
- Informer immédiatement le centre de services des ressources technologiques dans le cas d'un potentiel code malveillant reçu par courriel, Internet ou autres ;
- Accéder aux systèmes d'information avec le code utilisateur dont ils ont obtenu l'autorisation ;
- Utiliser les technologies de l'information de façon éthique et à des fins professionnelles seulement (dans le cadre de leurs fonctions), et de manière à préserver la mission et la réputation de l'organisme ;
- S'assurer de ne transmettre des informations confidentielles ou sensibles, en lien avec l'organisme, ses clients ou ses employés, que dans le cadre de leurs fonctions et en veillant à leur protection adéquate ;
- S'abstenir de modifier la configuration de leur poste de travail ou d'utiliser un logiciel non autorisé ;
- S'abstenir de tenter de contourner les mesures de sécurité mises en place.

7. ÉLABORATION, RÉDACTION ET MISE À JOUR DE LA POLITIQUE

7.1. Chef de Sécurité de l'Information Organisationnelle (CSIO)

Le CSIO est responsable de s'assurer de l'élaboration, de la rédaction et de la mise à jour de la politique.

7.2. Comité de sécurité de l'information

Les membres du comité de sécurité de l'information ont participé à l'élaboration et à la rédaction de la politique, et participent à sa mise à jour.

7.3. Calendrier de révision de la politique

La présente politique doit être révisée minimalement aux trois ans afin de s'assurer qu'elle est conforme aux lois, aux directives du Ministère de la Santé et des Services sociaux, du Secrétariat du Conseil du trésor et du Ministère de la Cybersécurité et de la Numérisation, aux nouvelles pratiques et aux technologies utilisées au sein du CIUSSS-EMTL.

8. LE CHEF DE LA SÉCURITÉ DE L'INFORMATION ORGANISATIONNEL (CSIO) DU CIUSSS-EMTL

Il est responsable de la mise en application de la présente politique.

9. ENTRÉE EN VIGUEUR

La présente politique entre en vigueur le jour de son adoption par le conseil d'administration du CIUSSS-EMTL et annule, par le fait même, toute autre politique en cette matière adoptée antérieurement dans l'une ou l'autre des installations administrées par le CIUSSS-EMTL.

10. ANNEXES

- ANNEXE I - Cadre légal et administratif de la sécurité de l'information;
- ANNEXE II - Positionnement de la Politique provinciale de sécurité de l'information;
- ANNEXE III - Cadre normatif de sécurité de l'information d'un organisme;
- ANNEXE IV – Définitions;
- ANNEXE V – Liste des acronymes.

ANNEXE I

Cadre légal et administratif de la sécurité de l'information

La présente politique s'inscrit principalement dans un contexte régit par les lois, codes et règlements suivants :

La loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, R.L.R.Q., c. G-1.03;

La Loi concernant le cadre juridique des technologies et l'information, R.L.R.Q., c. 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;

La Loi sur la protection des renseignements personnels dans le secteur privé;

La Loi sur la protection des renseignements personnels et les documents électroniques, LC 2000, c 5;

La Loi sur le droit d'auteur, L.R., 1985, c. C-42;

La loi sur les services de santé et les services sociaux, L.R.Q., c. S-4.2;

La loi modifiant l'organisation et la gouvernance du réseau de la santé et des services sociaux notamment par l'abolition des agences régionales, RLRQ c O-7.2;

La loi sur les services de santé et les services sociaux pour les autochtones cris, R.L.R.Q., c. S-5;

La loi sur les services préhospitaliers d'urgence, R.L.R.Q, c. S-6.2;

La Loi sur la Régie de l'assurance maladie du Québec, R.L.R.Q., c.R-5;

La Loi sur l'assurance maladie, R.L.R.Q., c. A-29, section VII;

La Loi médicale, R.L.R.Q., c. M-9;

La Loi sur la pharmacie, R.L.R.Q., c. P-10;

La Loi sur la santé publique, R.L.R.Q., c. S-2.2;

La Loi sur la protection de la jeunesse, R.L.R.Q., c. P-34.1;

La Loi sur le curateur public, R.L.R.Q., c. C-81;

La Loi sur la santé et la sécurité au travail, R.L.R.Q., c. S-2.1;

La Loi sur les accidents de travail et les maladies professionnelles, R.L.R.Q., c. A-3.001;

La Loi sur la recherche des causes et des circonstances de décès, R.L.R.Q., c. R-0.2;

Le Code des professions, R.L.R.Q., c. C-26, articles 60.4 à 60.6 et 87;

Les codes de déontologie des différents ordres professionnels oeuvrant dans le domaine de la santé et des services sociaux;

MSSS-POL01 Politique provinciale de sécurité de l'information 2015-03-02

Le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels, R.L.R.Q., c. A-2.1, r. 02;

La Charte des droits et libertés de la personne, R.L.R.Q., c. C-12;

Le Code civil du Québec, L.Q., 1991, c. 64;

La Loi sur les archives, R.L.R.Q., c. A-21.1;

La Loi sur l'administration publique, R.L.R.Q., c. A-6.01;

La Loi sur la fonction publique, R.L.R.Q., c. F-3.1.1;

La Loi canadienne sur les droits de la personne, L.R., 1985, c. H-6;

Le Code criminel, L.R., 1985, c. C-46;

La politique cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics;

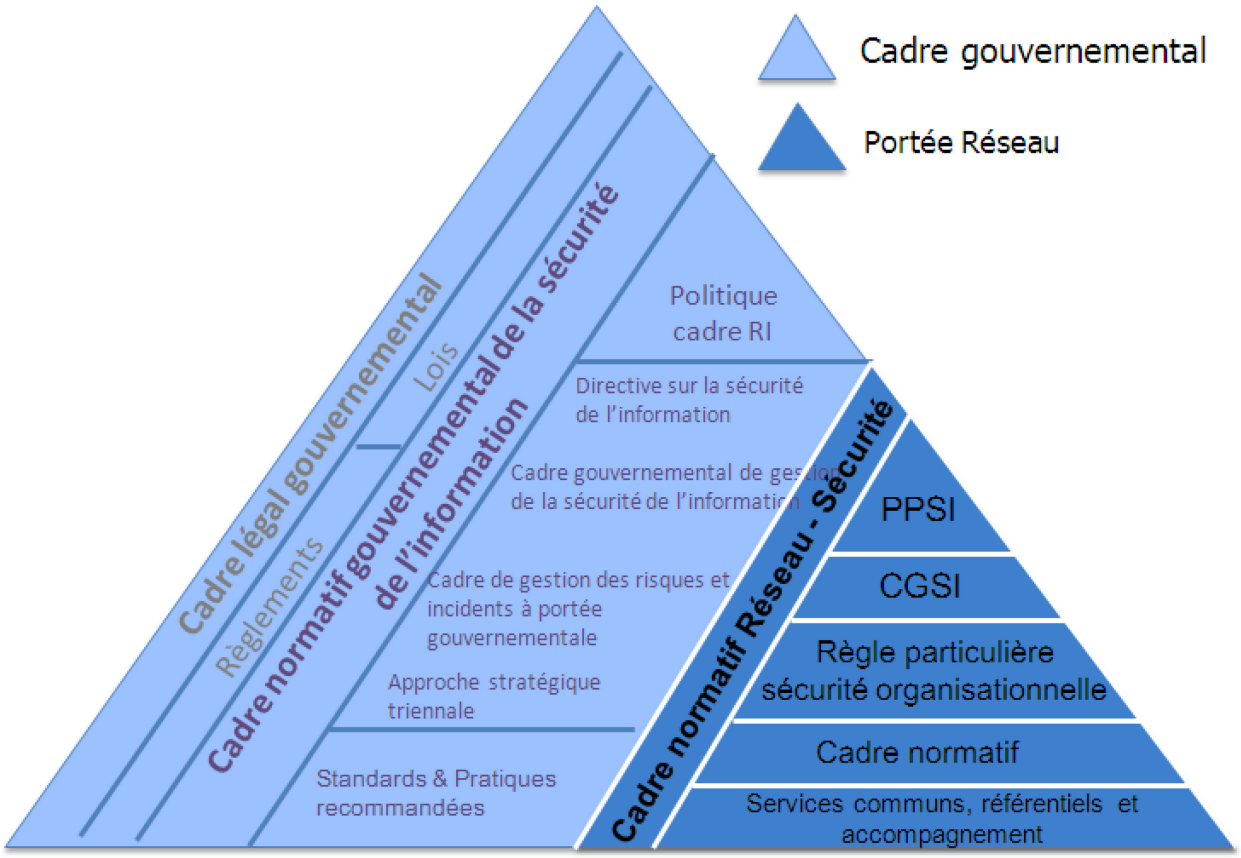
La Directive gouvernementale sur la sécurité de l'information, décret numéro 1514-2021 du 8 décembre 2021;

La Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (Loi 25).

ANNEXE II

Positionnement de la Politique provinciale de sécurité de l'information

La Politique provinciale de sécurité de l'information s'inscrit dans le cadre normatif du Réseau, tout en s'appuyant sur le cadre légal et normatif gouvernemental. Tel qu'illustré ci-dessous :



PPSI : Politique provinciale de sécurité de l'information
CGSI : Cadre de gestion de la sécurité de l'information

Source : *Politique provinciale sur la sécurité de l'information*, MSSS-POL01, Août 2015.

ANNEXE III

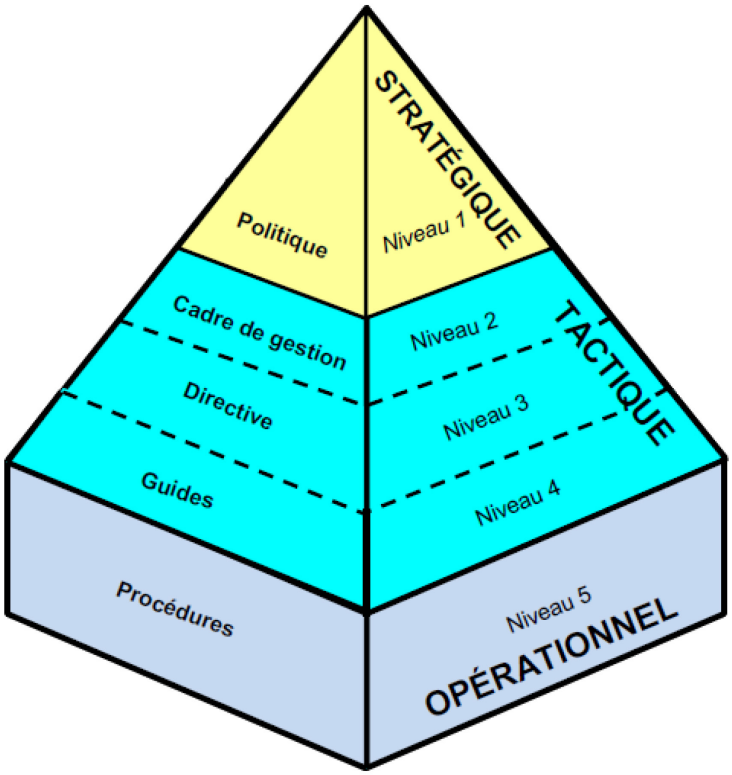
Cadre normatif de sécurité de l'information d'un organisme

Le schéma présenté ci-dessous illustre la hiérarchie des principales composantes du cadre normatif de sécurité de l'information d'un organisme.

Ces composantes se traduisent notamment :

- au niveau stratégique, par la politique de sécurité de l'information;
- au niveau tactique, par le cadre de gestion, les directives et les guides;
- au niveau opérationnel, par des procédures décrivant les étapes d'un processus d'implantation ou de mise en oeuvre d'une mesure de sécurité[16].

Structure du cadre normatif d'un organisme



Source : Guide d'élaboration d'un cadre de gestion de la sécurité de l'information, PR-075, Secrétariat du Conseil du Trésor, Juillet 2016.

[16] **Mesure de sécurité de l'information** : Moyen concret assurant, partiellement ou totalement, la protection d'un actif informationnel contre un ou plusieurs risques et dont la mise en oeuvre vise à amoindrir la probabilité de survenance de ces risques ou à réduire les pertes qui en résultent. Source : OQLF – Grand dictionnaire terminologique .

ANNEXE IV

Définitions

Continuité des services

Capacité d'une organisation d'assurer, en cas de sinistre, la poursuite de ses processus d'affaires selon un niveau de service prédéfini.

Directive

D'application obligatoire, une directive vise à préciser, pour un domaine d'application particulier de sécurité de l'information (sécurité des locaux et des équipements, échange sécuritaire de l'information, etc.), les dispositions à respecter aux fins d'assurer la sécurité de l'information. Mentionnons, à titre d'exemple, les directives portant sur la gestion des accès à l'information, les règles à adopter par les utilisateurs des assistants numériques personnels ou la protection des supports amovibles (mémoires Flash, disques durs, etc.).

Document [17]

Ensemble constitué d'information portée par un support. L'information y est délimitée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcriptibles sous l'une de ces formes ou en un autre système de symboles.

[...] est assimilée au document toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite.

Guide [18]

Les guides visent à faciliter l'application des prescriptions d'une politique, d'une directive ou éventuellement d'une norme, sans en avoir le caractère contraignant.

Mesure de sécurité de l'information [19]

Moyen concret assurant, partiellement ou totalement, la protection d'un actif informationnel contre un ou plusieurs risques et dont la mise en oeuvre vise à amoindrir la probabilité de survenance de ces risques ou à réduire les pertes qui en résultent.

Norme [20]

Accord entériné par un organisme officiel de normalisation comme l'Organisation internationale de normalisation (ISO), le Conseil canadien des normes (CCN), etc., contenant des spécifications techniques ou autres critères précis destinés à être utilisés systématiquement en tant que règles,

---

[17] *Loi concernant le cadre juridique des technologies de l'information - article 3.*
[18] *OQLF – Grand dictionnaire terminologique.*
19 Ibid.
20 Lexique gouvernemental.

lignes directrices ou définitions de caractéristiques pour assurer que des matériaux, produits, processus et services sont aptes à leur emploi.

Organisme

Le ministère de la Santé et des Services sociaux, les centres intégrés de santé et de services sociaux et les autres entités du réseau de la santé et des services sociaux.

Pratique [21]

Savoir ou manière de faire qui, dans une organisation, conduisent au résultat souhaité et qui sont portés en exemple auprès des pairs afin de leur faire partager l'expérience qui leur permettra une amélioration collective.

Procédure

Une procédure est un ensemble d'étapes à franchir, de moyens à prendre et de méthodes à suivre dans l'exécution d'une tâche. Elle décrit en détail les étapes d'un processus humain ou technologique d'implantation ou d'application d'une mesure de sécurité, qu'elle soit administrative ou technologique. Citons, à titre d'exemple, les procédures se rapportant à la délivrance ou la révocation des cartes d'accès, à la destruction sécuritaire des documents administratifs ou à l'attribution des mots de passe.

Processus

Suite cohérente d'activités et d'opérations d'une organisation traduisant les besoins de la clientèle et des employés dans une logique de création de valeur.

Renseignement personnel [22]

Tout renseignement qui concerne une personne physique et permet 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.

Note[23] : Les renseignements personnels suivants ont un caractère public : le nom, le titre, la fonction, la classification, le traitement, les coordonnées du lieu de travail d'un membre d'un organisme public, de son conseil d'administration ou de son personnel de direction.

Ressources informationnelle

Les actifs informationnels ainsi que les ressources humaines, matérielles et financières directement affectées à la gestion, à l'acquisition, au développement, à l'entretien, à l'exploitation, à l'accès, à l'utilisation, à la protection, à la conservation et à l'aliénation de ces actifs.

Standard

Norme qui n'a été ni définie ni entérinée par un organisme officiel de normalisation comme l'Organisation internationale de normalisation (ISO), le Conseil canadien des normes (CCN), etc.,

---

[21] *Inspirée de l'OQLF – Grand dictionnaire terminologique.*
[22] *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels,* RLRQ c A-2.1 *[Loi sur l'accès]*
[23] *Ibid., ,* art 57 (1)

mais qui s'est imposée par la force des choses parce qu'elle fait consensus auprès des utilisateurs, d'un groupe d'entreprises ou encore d'un consortium.

Sources (sauf si autrement indiqué): *Politique provinciale sur la sécurité de l'information*, MSSS-POL01, Août 2015; *Cadre de gestion de la sécurité de l'information,* MSSS-CDG01, Août 2015; Guide d'élaboration d'un cadre de gestion de la sécurité de l'information, PR-075, Secrétariat du Conseil du Trésor, Juillet 2016.

ANNEXE V

Liste des acronymes

Directions

CSI : Centre de Services Informatiques

DRT : Direction des Ressources Technologiques

DRH : Direction des Ressources Humaines et Direction des Communications

DST : Direction des Services Techniques

RITM : Réseau Intégré de Télécommunications Multimédia

Organisations

CEMTL : CIUSSS de l'Est-de-l'Ile-de-Montréal

COCD : Centre Opérationnel de Cyberdéfense

MCN : Ministère de la Cybersécurité et de la Numérisation

MSSS : Ministère de la Santé et des Services Sociaux

RSSS : Réseau de la Santé et des Services Sociaux

SCT : Secrétariat du Conseil du Trésor

Rôles

CA : Conseil d'Administration

CD : Comité de Direction

COMSI : Coordonnateur organisationnel des mesures de sécurité de l'information

CR : Comité de Révision

CSIO : Chef de Sécurité de l'Information Organisationnelle

DO : Dirigeant de l'Organisation

DPI : Dirigeant Principal de l'Information

DRI : Dirigeant de Réseau de l'Information

RH : Ressources Humaines

SOC : Centre d'Opérations de Sécurité (Security Operations Centers)

Termes liés à la sécurité de l'information

Cote D.I.C : Disponibilité, Intégrité, Confidentialité

CGSI : Cadre de Gestion de la Sécurité de l'Information

DAI : Détenteurs des Actifs Informationnels

GIR : Gestion Intégrée des Risques

PRP : Protection des Renseignements Personnels

SI : Sécurité de l'Information

TI : Technologie de l'Information