Centre intégré universitaire de santé et de services sociaux du Saguenay–Lac-Saint-Jean
Québec

Politique

Politique de sécurité de l'information

N° d'identification : PO-RI.004

Procédure(s) associée(s) à la politique : À venir

CE DOCUMENT S'ADRESSE AUX PERSONNES SUIVANTES :	
Toute personne physique ou morale œuvrant dans l'établissement	
CE DOCUMENT EST ACCESSIBLE :	
☐Répertoire commun ☐Site Internet ☒ Intranet ☐Autre précisez :	
NOMBRE DE PAGES	7
RESPONSABLE DE L'APPLICATION	Responsable de la sécurité de l'information
RESPONSABLE DE LA CODIFICATION ET DE LA CONSERVATION DU DOCUMENT	Direction des ressources humaines, des communications et des affaires juridiques
INSTANCE(S) CONSULTÉE(S) RÉFÉRENCES	La politique provinciale sur la sécurité de l'information (MSSS-POL01) Le cadre de gestion de la sécurité de l'information (MSSS-CDG01)
RESPONSABLE DE L'ADOPTION OU DE LA RÉVISION FINALE	Conseil d'administration
DATE DE LA MISE EN VIGUEUR	23 mars 2016
DATE DE L'ADOPTION OU DE LA RÉVISION ET NUMÉRO DE RÉSOLUTION DU C.A.	23 mars 2016
RÉVISION	Novembre 2020

1. Principes directeurs

La modernisation du réseau de la santé et des services sociaux repose sur la possibilité de s'échanger des informations de façon rapide et sécuritaire. L'intégration de plus en plus grande des systèmes d'information à la majorité des activités de l'établissement favorise l'accessibilité à des renseignements de toute nature par les intervenants dûment autorisés. Cette intégration contribue toutefois à augmenter les probabilités d'accroissement des manquements au respect de la confidentialité des données des usagers.

Le Centre intégré universitaire de santé et de services sociaux (CIUSSS) du Saguenay–Lac-Saint-Jean reconnaît que l'information est essentielle à ses opérations courantes et, de ce fait, qu'elle doit faire l'objet d'une évaluation, d'une utilisation appropriée et d'une protection adéquate. L'établissement reconnaît détenir, en outre, des renseignements personnels ainsi que des informations qui ont une valeur clinique, légale, administrative ou économique.

2. Cadre juridique

Plusieurs lois et directives encadrent et régissent l'utilisation de l'information. L'établissement est assujetti à ces lois et doit s'assurer du respect de celles-ci. En conséquence, l'établissement met en place la présente politique de sécurité de l'information qui oriente et détermine l'utilisation appropriée et sécuritaire de l'information et des technologies de l'information.

La présente politique est également adoptée en application du paragraphe (a) du premier alinéa de l'article 7 de la Directive sur la sécurité de l'information gouvernementale du Secrétariat du Conseil du trésor (SCT), décret 7-2014, qui confère aux organismes relevant du dirigeant réseau de l'information de nouvelles obligations en matière de sécurité de l'information, de protection des renseignements personnels et de respect de la vie privée.

3. Objectif

La présente politique sert de fondation en matière de sécurité de l'information dans l'établissement et a pour but de définir une gouverne claire, forte et intégrée en la matière, conformément aux lois et aux règlements applicables afin d'assurer la disponibilité, l'intégrité et la confidentialité de l'information.

La politique de sécurité de l'information permet d'affirmer l'engagement de l'établissement de s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information. Elle permet au responsable de la sécurité de l'information de définir un ensemble de principes visant à :

3.1 Structurer la prise en charge de la sécurité de l'information au sein de l'établissement.

3.2 Assurer la disponibilité, l'intégrité et la confidentialité à l'égard de l'utilisation des réseaux informatiques, de télécommunication sociosanitaire et d'Internet, de l'utilisation des actifs informationnels et des télécommunications ainsi que des données corporatives.

3.3 Protéger les informations des usagers.

3.4 Assurer le respect de la vie privée des individus, notamment la confidentialité des renseignements à caractère nominatif relatifs aux usagers et au personnel de l'établissement tout au long de son cycle de vie.

3.5 Assurer, par conséquent, le respect des données confidentielles, des données relatives à la propriété intellectuelle ou encore, des renseignements de toute nature concernant une recherche, lesquels sont qualifiés de strictement confidentiels avec ou sans l'utilisation des actifs informationnels et de télécommunication.

Tous les documents d'encadrement doivent présenter les objectifs puisqu'ils permettent de savoir pourquoi on élabore ledit document.

4. Champs d'application

L'information visée par la présente politique est celle que l'établissement détient dans l'exercice de sa mission, que sa conservation soit assurée par lui-même ou par un tiers, quelle que soit son support ou son moyen de communication, et ce, tout au long de son cycle de vie.

La présente politique s'applique à :

4.1 toute personne physique ou morale œuvrant au sein de l'établissement qui utilise ou accède aux informations de l'organisation, quel que soit le support sur lequel elles sont conservées. Citons à titre d'exemple, tout le personnel de l'établissement incluant les médecins, les résidents, les organismes partenaires, les bénévoles, les stagiaires, les contractuels et les fournisseurs de services.

4.2 l'ensemble des actifs informationnels ainsi qu'à leur utilisation au sein de l'établissement, tels que les banques d'information électronique, les informations papier ou autres et les données sans égard aux médiums de support, les réseaux et équipements de communication, les systèmes d'information, les logiciels, les équipements informatiques ou centres de traitement utilisés par l'établissement, de même que toute la gestion et la disposition des documents et des informations qu'ils contiennent;

4.3 l'ensemble des activités en gestion des ressources informationnelles, collecte, enregistrement, traitement, garde, conservation, diffusion et autres;

4.4 toute situation qui pourrait permettre de voir ou d'entendre des informations à caractère confidentiel de façon accidentelle ou non;

4.5 aux contrats et ententes de service avec tout intervenant externe. Les ententes doivent contenir les dispositions requises pour garantir le respect de la présente politique et les directives et procédures qui en découlent.

5. Définitions

Actif informationnel : actif informationnel au sens de la Loi concernant 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'établissement.

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

Gestion intégrée des risques de sécurité : 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.

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.

Réseau : ensemble des organismes qui relèvent du Dirigeant réseau de l'information (DRI) de la santé et des services sociaux en vertu de l'article 2, paragraphe 5 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LGGRI).

Risque de sécurité de l'information : probabilité que survienne un événement préjudiciable, plus ou moins prévisible, qui peut affecter la réalisation des objectifs de l'organisme ou du Réseau.

6. Respect de la politique

L'établissement exige de toutes les personnes énumérées précédemment dans la rubrique « champ d'application » de se conformer aux dispositions de la présente politique ainsi qu'aux directives et procédures qui s'y rattachent.

L'établissement oblige également la signature d'un engagement à la confidentialité (voir en annexe) par tous les utilisateurs, et ce, dès l'embauche, par l'intermédiaire des ressources humaines.

7. Énoncés et principes généraux

Le président-directeur général (PDG) reconnaît que la gouvernance de la sécurité de l'information est basée sur une prise en charge engagée et imputable mettant en avant-plan l'amélioration continue, la proactivité et la reddition de comptes à tous les niveaux hiérarchiques, tout en favorisant une collaboration soutenue avec les différents intervenants, la sensibilisation, le partage et le renforcement des connaissances.

Toute personne au sein du Centre intégré universitaire de santé et de services sociaux du Saguenay–Lac-Saint-Jean ayant accès aux actifs informationnels assume des responsabilités spécifiques en matière de sécurité et est redevable de ses actions auprès de la Direction de l'établissement.

Des mesures de protection, de prévention, de détection et de correction, ainsi que des mesures disciplinaires, doivent être mises en place afin d'assurer la sécurité des actifs informationnels appartenant à l'établissement. Ces mesures visent à assurer :

- la disponibilité, laquelle est la propriété d'une information d'être accessible et utilisable en temps voulu et de manière adéquate par une personne autorisée;
- l'intégrité, laquelle est la propriété d'une information ou d'une technologie de l'information de n'être ni modifiée, ni altérée, ni détruite sans autorisation;
- la confidentialité, laquelle est la propriété d'une information d'être accessible aux seules personnes autorisées;
- l'authentification, laquelle est une fonction permettant d'établir la validité de l'identité d'une personne ou d'un dispositif;
- l'irrévocabilité, laquelle est la propriété d'un acte d'être définitif et clairement attribué à la personne qui l'a accompli ou au dispositif avec lequel cet acte a été accompli.

Ces mesures doivent notamment empêcher les accidents, l'erreur, la malveillance et la destruction des informations sans autorisation.

8. Structure fonctionnelle

La structure fonctionnelle de la sécurité de l'information de l'établissement ainsi que les rôles et responsabilités des principaux intervenants en sécurité de l'information sont définis dans le cadre de gestion de la sécurité de l'information (CGSI) qui vient compléter les dispositions de la présente politique locale.

Le président-directeur général est l'ultime responsable de la sécurité de l'information relevant de son autorité. À ce titre, il prend les moyens nécessaires à la mise en œuvre et à la gestion de la sécurité de l'information de son organisme.

Il est également responsable devant le ministre de la Santé et des Services sociaux 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 tout contrat signé avec un partenaire interne ou externe.

Toute personne autorisée à avoir accès aux actifs informationnels du CIUSSSS du Saguenay–Lac-Saint-Jean assume des responsabilités particulières en matière de sécurité de l'information, notamment en matière de protection de l'information, et répond de ses actions auprès du PDG de l'établissement.

Le responsable de la sécurité de l'information assiste le PDG dans la détermination des orientations stratégiques et des priorités d'intervention.

9. Droit de regard

Le président-directeur général ou le responsable de la sécurité de l'information qu'il a désigné exerce, en conformité avec la législation et la réglementation en vigueur, un droit de regard sur tout usage des actifs informationnels de l'établissement.

Des mécanismes sont mis en place pour permettre à l'établissement de démontrer une prise en charge maîtrisée de la sécurité de l'information, conformément à la directive sur la sécurité de l'information gouvernementale.

10. Sanctions

Lorsqu'un utilisateur ou une organisation contrevient ou déroge à la présente politique ou aux directives et procédures et tout autre document en découlant, il s'expose, selon le cas, à des mesures disciplinaires, administratives ou légales en fonction de la gravité de son geste. Ces mesures peuvent inclure la suspension des privilèges relatifs à l'accès aux actifs informationnels, la réprimande, la suspension ou le congédiement.

11. Dispositions finales

La présente politique est réévaluée minimalement aux trois ans par la Direction des ressources informationnelles. Elle entre en vigueur à la date de son approbation par le conseil d'administration de l'établissement.

Centre intégré universitaire de santé et de services sociaux du Saguenay–Lac-Saint-Jean
Québec

Engagement à la confidentialité et au respect de la politique de sécurité de l'information

JE, soussigné(e), (prénom, nom) _____ **CONFIRME** avoir reçu copie de la politique relative à la sécurité de l'information du CIUSSS du Saguenay–Lac-Saint-Jean.

JE M'ENGAGE à prendre connaissance, respecter cette politique et à appliquer ses lignes de conduite dans le but de préserver la sécurité et l'intégrité des actifs informationnels ainsi que d'assurer la confidentialité des données qui s'y trouvent.

JE SUIS PLEINEMENT CONSCIENT(E) que le CIUSSS du Saguenay–Lac-Saint-Jean exerce une surveillance des systèmes d'information. J'ai également été informé(e) que les systèmes d'information du CIUSSS enregistrent les coordonnées permettant à l'établissement de visualiser, par un système de journalisation, l'historique des accès aux données que je consulte.

JE RECONNAIS que les systèmes d'information sont des outils de travail qui doivent être utilisés uniquement dans le cadre de mes fonctions ou des activités de l'établissement et conformément à la présente politique. L'utilisation des systèmes d'information à des fins personnelles ou d'une manière non conforme à la politique est donc strictement interdite. Compte tenu de tout ce qui précède, rien dans l'utilisation des systèmes d'information ne doit être considéré comme étant confidentiel ou faisant partie de la vie privée.

JE SUIS ÉGALEMENT CONSCIENT(E) que tout manquement au respect à la confidentialité, ou tout acte mettant en péril la sécurité des actifs informationnels, tel que stipulé dans la politique de sécurité de l'information, peut occasionner des sanctions telles que définies dans la politique.

JE CONFIRME avoir été informé(e) de l'obligation de respecter la confidentialité, sauf dans les cas prévus par la loi, de toutes les informations que je pourrai voir, entendre ou recueillir dans le cadre de mes fonctions, tel que stipulé dans le Code d'éthique du CIUSSS, ceci conformément à la Loi sur les services de santé et les services sociaux, au Code civil du Québec et à la Charte des droits et libertés de la personne.

JE M'ENGAGE à informer, sans délai, mon supérieur immédiat de tout incident susceptible de compromettre la confidentialité ou la sécurité des renseignements confidentiels.

JE M'ENGAGE ÉGALEMENT à limiter la consultation des renseignements confidentiels aux seules fins d'accomplissement de mes fonctions et à ne jamais dévoiler ces renseignements confidentiels à quiconque.

JE DÉCLARE AVOIR LU ET COMPRIS le contenu de cet engagement à la confidentialité et **JE M'ENGAGE** à m'y conformer en tout temps.

Cette déclaration solennelle me lie à perpétuité, et ce, même après la cessation de mon emploi ou de mes activités au CIUSSS du Saguenay–Lac-Saint-Jean.

(Veuillez cocher la case appropriée)

☐ employé ☐ médecin ☐ résident ☐ stagiaire ☐ étudiant ☐ recherche ☐ bénévole
☐ contractuel ☐ Fournisseur

Nom et prénom de la personne qui œuvre au CIUSSS du Saguenay–Lac-Saint-Jean (LETTRES CARRÉES)	Numéro d'employé	Numéro de pratique
Signature de la personne	Date	
Signature du représentant du CIUSSS du Saguenay–Lac-Saint-Jean	Date	

Québec