CENTRE RÉGIONAL DE SANTÉ ET DE SERVICES SOCIAUX DE LA BAIE-JAMES

Nº 3.8

POLITIQUE	**DÉPARTEMENT : DIRECTION DES RESSOURCES FINANCIÈRES, TECHNIQUES ET INFORMATIONNELLES**	
SÉCURITÉ DE L'INFORMATION		**Version nº** 3
Destinataire : Toute personne à l'emploi du CRSSS de la Baie-James, médecins ou toute personne physique ou morale		
Responsable de l'application : Présidente-directrice générale		
Signature : LU ET APPROUVÉ PAR Présidente-directrice générale		14 mars 2017 Date

1. PRÉAMBULE, OBJECTIF ET BUTS

Dans l'accomplissement de sa mission, le centre régional de santé et de services sociaux de la Baie-James traite de l'information sous plusieurs formes et sur plusieurs supports à l'aide de différents systèmes d'information. Cette information détenue par l'établissement afin de soutenir ses activités possède une valeur administrative, légale ou financière et doit, par conséquent, faire l'objet d'une évaluation continue, d'une utilisation appropriée et d'une protection adéquate tout au long de son cycle de vie.

La présente politique sert de fondation en matière de sécurité de l'information dans l'établissement et soutient la mise en oeuvre du cadre de gestion en matière de sécurité de l'information et renforce le maintien de systèmes de contrôles internes offrant une assurance raisonnable de conformité à l'égard des lois, directives et pratiques gouvernementales en la matière.

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

- Structurer la prise en charge de la sécurité de l'information au sein de l'établissement;
- 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;
- Protéger les informations des usagers;
- 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;
- 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.

2. CADRE JURIDIQUE

La Politique de sécurité de l'information s'inscrit notamment dans un contexte régi par :

- La loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, L.R.Q., c. G-1.03;
- La Loi concernant le cadre juridique des technologies et l'information, L.R.Q., c. C-1.1;
- La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, L.R.Q., c. A-2.1;
- La Loi sur la protection des renseignements personnels et les documents électroniques;
- 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;
- La loi sur les services de santé et les services sociaux pour les autochtones cris, L.R.Q., c. S-5;
- La loi sur les services préhospitaliers d'urgence, L.R.Q, c. S-6.2;
- La Loi sur la santé publique, L.R.Q., c. S-2.2;
- La Loi sur la protection de la jeunesse, L.R.Q., c. P-34.1;
- La Loi sur le curateur public, L.R.Q., c. C-81;
- Le Code des professions, 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;
- Le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels, c. A-2.1, r. 02;
- La Charte des droits et libertés de la personne, L.R.Q., c. C-12;
- Le Code civil du Québec, L.Q., 1991, c. 64;
- La Loi sur les archives, L.R.Q., c. A-21.1;
- La Loi sur l'administration publique, L.R.Q., c. A-6.01;
- La Loi sur la fonction publique, 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 sur la sécurité de l'information gouvernementale, décret 7-2014.

3. 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, quels que soient son support ou son moyen de communication, et ce, tout au long de son cycle de vie.

La présente politique s'applique à :

- 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 ;
- L'ensemble des actifs informationnels ainsi qu'à leur utilisation au sein de l'établissement, tel 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;
- L'ensemble des activités en gestion des ressources informationnelles, collecte, enregistrement, traitement, garde, conservation, diffusion et autres;
- Toute situation qui pourrait permettre de voir ou d'entendre des informations à caractère confidentiel de façon accidentelle ou non;
- 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.

4. DÉFINITIONS ET ABRÉVIATIONS

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.

CRSSS : Centre régional de santé et de services sociaux

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.

Irrévocabilité: propriété d'un acte d'être définitif et qui est clairement attribué à la personne qui l'a posé ou au dispositif avec lequel cet acte a été accompli.

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.

5. PRINCIPES DIRECTEURS

Les principes directeurs permettront d'assurer les objectifs du présent document. Ces principes s'articulent autour de la sécurité de l'information, et leur transmission et de l'accès aux données ou à une information.

- Le président-directeur général de l'établissement 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 oeuvre et à la gestion de la sécurité de l'information de son organisme.
- Tous les utilisateurs des actifs informationnels ainsi que toutes les personnes visées qui ont accès à un actif de l'établissement doivent signer une déclaration d'allégeance.
- Les renseignements personnels ne doivent être utilisés ou ne servir qu'aux fins pour lesquelles ils ont été recueillis ou obtenus.
- Les incidents ayant pu mettre ou ayant mis en péril la sécurité de l'information doivent être déclarés et consignés dans un registre.
- 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.

- Un programme continu de sensibilisation et de formation à la sécurité informatique doit être mis en place à l'intention du personnel, des administrateurs de l'établissement ou de toute autre personne physique ou morale agissant pour le compte de l'établissement.

6. STRUCTURE FONCTIONNELLE

6.1 Responsabilités des différents intervenants

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) du CRSSS de la Baie-James qui vient compléter les dispositions de la présente politique locale.

6.2 Responsabilités de l'application

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 CRSSS de la Baie-James 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 président-directeur général de l'établissement.

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

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.

6.3 Respect de la politique

L'établissement exige de toutes les personnes énumérées précédemment dans la rubrique « champs 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 par tous les utilisateurs, et ce, dès l'embauche, par l'intermédiaire des ressources humaines.

Lorsqu'un utilisateur ou une organisation contrevient ou déroge à la présente politique ou aux directives et procédures et tous les autres documents en découlant, il s'expose, selon le cas, à des mesures disciplinaires, administratives ou légales en fonction de la gravité de son geste.

7. ENTRÉE EN VIGUEUR

La politique entre en vigueur à compter de la date de signature de la personne autorisée.

8. BIBLIOGRAPHIE

CONSEIL DU TRÉSOR. *Directive sur la sécurité de l'information gouvernementale, Décret 7-2014* [recueil des politiques de gestion du MSSS 11-2-2-2], Québec, [Ministère de la santé et des service sociaux], 23 janvier 2014;

CONSEIL DU TRÉSOR. *Approche stratégique gouvernementale 2014-2017 Sécurité de l'information,* juin 2014, 24 p

Centre intégré universitaire de santé et de services sociaux (CIUSSS) du Saguenay-Lac-Saint-Jean. Politique de sécurité de l'information, DRI 503, 23 mars 2016;

MINISTÈRE DE LA SANTÉ ET DES SERVICES SOCIAUX. Cadre de gestion de la sécurité de l'information (MSSS-CDG01), août 2015, 15 p.

MINISTÈRE DE LA SANTÉ ET DES SERVICES SOCIAUX. Politique provinciale de la sécurité de l'information MSSS-POL01, août 2015, 10 p.

9. LISTE DES MODIFICATIONS ET COMMENTAIRES

DATE aaaa-mm-jj	VERSION	MODIFICATIONS/COMMENTAIRES	ARCHIVÉ
2017-03-14	**3**	Changement de titre des directions	

10 RÉVISION ANNUELLE

La personne soussignée a revu ce document à la date indiquée et l'a reconduit sans modification.

DATE	SIGNATURE AUTORISÉE