Centre intégré universitaire de santé et de services sociaux de la Capitale-Nationale Québec	**POLITIQUE**
	Code : PO-13
	Direction responsable : Direction des ressources informationnelles
	Adoptée par le comité de direction le : 25 octobre 2016
	Adoptée par le conseil d'administration le : 8 novembre 2016
	Entrée en vigueur le : 9 novembre 2016

TITRE : Politique relative à la sécurité de l'information

CONSULTATIONS	
☐ Conseil des infirmières et infirmiers :	☐ Cadres :
☐ Conseil multidisciplinaire :	☐ Autres :
☐ Conseil des médecins, dentistes et pharmaciens :	

1. PRINCIPES

La politique de sécurité du Centre intégré universitaire de santé et de services sociaux de la Capitale-Nationale (CIUSSS de la Capitale-Nationale) est fondée sur le Cadre global de gestion des actifs informationnels – volet sécurité (CGGAI) adopté par le Ministère de la Santé et des services sociaux (MSSS) ainsi que les politiques et cadres de gestion du MSSS qui en découlent.

2. OBJECTIFS

La politique de sécurité de l'information sert de fondation en matière de sécurité de l'information et permet au Président directeur général de définir un ensemble de principes visant à :

- structurer la prise en charge de la sécurité de l'information au sein de l'organisme;
- assurer la conformité aux lois et règlements applicables ainsi que les directives, normes et orientations gouvernementales notamment en matière de reddition de comptes;
- assurer la disponibilité, l'intégrité et la confidentialité de l'information de l'établissement, tout au long de son cycle de vie :
    - assurer le respect des cinq grands axes de disponibilité, intégrité et confidentialité de l'actif informationnel (DICAI) tout au long du cycle de vie, de tous les actifs informationnels détenus ou sous sa responsabilité;
    - assurer l'authentification des personnes accédant à l'information de l'établissement et la traçabilité de façon irrévocable, des actes qu'elles posent sur cette information;
- protéger les informations des usagers de l'établissement et des personnes qui exercent leur fonction ou leur profession au sein de l'établissement;
- développer la mise en place d'une culture en matière de sécurité de l'information.

3. CHAMP D'APPLICATION

Cette politique s'applique à toute personne physique ou morale qui utilise ou peut avoir accès à un ou plusieurs actifs informationnels, peu importe l'endroit où elle se trouve ou la localisation de l'actif.

L'information visée par la présente politique est celle que le CIUSSS de la Capitale-Nationale détient dans l'exercice de sa mission, que sa conservation soit assurée par lui-même ou par un tiers.

4. DÉFINITIONS

Pour la présente politique, les termes et expressions suivantes signifient :

- **Actif informationnel :** Actif informationnel au sens de la 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.

- **Authentification :** Acte permettant d'établir la validité de l'identité d'une personne ou d'un dispositif.

- **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.

- **Détenteur :** Un employé désigné par son organisme public, appartenant à la classe d'emploi de niveau-cadre ou à une classe d'emploi de niveau supérieur, et dont le rôle est notamment de s'assurer de la sécurité de l'information et des ressources qui la sous-tendent relevant de la responsabilité de son unité administrative.

- **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 explicitement attribué à la personne qui l'a posé ou au dispositif avec lequel cet acte a été accompli.

- **Renseignements personnels :** Sont personnels les renseignements qui concernent une personne physique et permettent de l'identifier. Le nom d'une personne physique n'est pas un renseignement personnel, sauf lorsqu'il est mentionné avec un autre renseignement la concernant ou lorsque sa seule mention révélerait un renseignement personnel concernant cette personne.

- **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'établissement ou du Réseau.

- **Utilisateur :** Toute personne physique ou morale, groupe ou entité administrative qui fait usage d'un ou de plusieurs actifs informationnels sous la responsabilité de l'établissement. Notamment, les stagiaires, les résidents, les externes, les chercheurs, les médecins, le personnel et les tiers, etc.

5. MODALITÉS

5.1 Énoncés et principes généraux

Le Président directeur général 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.

5.2 Responsabilité et imputabilité

5.2.1 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 l'établissement.

5.2.2 L'établissement 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.

5.2.3 Toute personne, autorisée à avoir accès aux actifs informationnels de l'établissement assume des responsabilités particulières en matière de sécurité de l'information, notamment en terme de protection de l'information, et répond de ses actions auprès du Président directeur général.

5.3 Approche globale de la sécurité de l'information

5.3.1 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.

5.3.2 La gestion de la sécurité demande la mise en place d'un ensemble de mesures coordonnées, adaptées à la nature de l'organisme, supportant les besoins d'affaires, encadrées par des exigences de sécurité et des pratiques reconnues, tout en laissant le choix des moyens de mise en œuvre à l'organisme.

5.4 Gestion intégrée des risques de sécurité de l'information

5.4.1 La gestion intégrée des risques de sécurité de l'information est une responsabilité organisationnelle qui requiert la mise en place d'un système, basé sur un principe d'amélioration continue et qui permet l'identification, l'analyse et le traitement des risques de sécurité à tous les niveaux hiérarchiques.

5.4.2 L'établissement évalue sur une base régulière et dans le cadre de projets d'informatisation, les risques d'atteinte à la disponibilité, l'intégrité et la confidentialité de l'information, pouvant affecter la réalisation de leurs missions et mettre en place des mesures permettant de réduire ces risques.

5.4.3 L'établissement met en œuvre des processus de gestion de la sécurité de l'information qui assurent le respect des exigences de sécurité de l'information, ainsi que l'adoption de pratiques recommandées en sécurité de l'information.

5.4.4 Tout manquement à la sécurité de l'information fait l'objet d'une vérification afin de rendre compte de la situation au responsable de la sécurité de l'information de l'établissement et d'appliquer les correctifs appropriés.

5.5 Sensibilisation et formation

5.5.1 La sensibilisation et la formation du personnel en sécurité de l'information sont indispensables à l'implantation d'une culture de sécurité.

5.5.2 Les principaux intervenants en sécurité de l'information et les gestionnaires reçoivent une formation et le soutien nécessaire pour s'assurer qu'ils maîtrisent les concepts de base en sécurité de l'information et prennent des décisions éclairées.

5.5.3 L'établissement effectue, sur une base régulière, des activités de sensibilisation et de formation de leurs utilisateurs à la sécurité de l'information, aux conséquences d'une atteinte à la sécurité de l'information, ainsi qu'à leurs rôles et leurs obligations en cette matière.

5.6 Droit de regard

5.6.1 Le ministre de la Santé et des Services sociaux exerce, en conformité avec la législation et la réglementation en vigueur, un droit de regard sur tout usage des actifs informationnels du Réseau.

5.6.2 Des mécanismes sont mis en place pour permettre aux organismes du Réseau de démontrer au ministre de la Santé et des Services sociaux, une prise en charge maîtrisée de la sécurité de l'information à leur niveau organisationnel, conformément à la directive sur la sécurité de l'information gouvernementale.

5.7 Sanctions

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

6. RESPONSABILITÉS

La structure fonctionnelle de la sécurité de l'information du Réseau 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. La section 7.2 du Cadre de gestion de la sécurité de l'information y définit les responsabilités des intervenants et l'organisme en matière de sécurité informationnelle soit :

- Le conseil d'administration
- Le Président directeur général
- Le responsable de la sécurité de l'information (RSI)
- Le conseiller en gouvernance de la sécurité de l'organisme
- L'officier de sécurité de l'information
- Le comité de sécurité de l'information de l'organisme
- Les responsables de domaines connexes à la sécurité de l'information
- Les détenteurs de l'information
- Les gestionnaires
- Les utilisateurs

7. ENTRÉE EN VIGUEUR

8. ANNEXES

Annexe 1 : Cadre légal et administratif

ANNEXE 1

Cadre légal et administratif

La présente politique s'inscrit principalement dans un contexte régit 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 dans le secteur privé;
- 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 Régie de l'assurance maladie du Québec, L.R.Q., c. R-5;
- La Loi sur l'assurance maladie, L.R.Q., c. A-29, section VII;
- La Loi médicale, L.R.Q., c. M-9;
- La Loi sur la pharmacie, L.R.Q., c. P-10;
- 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;
- La Loi sur la santé et la sécurité au travail, L.R.Q., c. S-2.1;
- La Loi sur les accidents de travail et les maladies professionnelles, L.R.Q., c. A-3.001;
- La Loi sur la recherche des causes et des circonstances de décès, L.R.Q., c. R-0.2;
- Le Code des professions, L.R.Q., c. C-26, articles 60.4 et 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.