Centre intégré universitaire de santé et de services sociaux de la Capitale-Nationale Québec	**POLITIQUE**
	Code : PO-13
	Direction responsable : Direction des ressources informationnelles
	Approuvée par le comité de direction le : 25 octobre 2016 et 9 janvier 2024
	Adoptée par le conseil d'administration le : 8 novembre 2016 Révisée le : 6 février 2024
	Résolution no. : CA-CIUSSS-2024-02[PO-13]-06 Entrée en vigueur le : 9 novembre 2016
TITRE : Politique relative à la sécurité de l'information	

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

1. PRINCIPES

La politique relative à la sécurité de l'information du Centre intégré universitaire de santé et de services sociaux de la Capitale-Nationale (CIUSSS de la Capitale-Nationale) est fondée sur la Politique gouvernementale de cybersécurité adoptée par le Secrétariat du Conseil du Trésor en mars 2020, sur la Politique provinciale de sécurité de l'information adoptée en septembre 2022 par le ministère de la Santé et des Services sociaux (MSSS), sur la Directive gouvernementale sur la sécurité de l'information (décret numéro 1514-202) ainsi que les politiques et cadres de gestion du MSSS qui en découlent.

2. OBJECTIFS

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

- Structurer la prise en charge de la sécurité de l'information au sein de l'établissement afin de s'assurer que le personnel et les parties prenantes sont conscients et tenus informés de leurs responsabilités en matière de sécurité de l'information;
- Assurer la conformité aux lois et règlements applicables ainsi que les directives, normes et orientations gouvernementales, notamment en matière de reddition de comptes;
- Assurer le respect des cinq grands axes à savoir : la disponibilité, l'intégrité, la confidentialité, l'authentification et l'irrévocabilité tout au long du cycle de vie, de tous les actifs informationnels détenus ou sous sa responsabilité;
- 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 afin que tous prennent en compte la sécurité de l'information dans leur activité quotidienne.

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 Loi concernant le partage de certains renseignements de santé, 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.

- **Catégorisation :** Processus permettant de déterminer le niveau de criticité des actifs informationnels, compte tenu de l'impact que peut engendrer un bris de disponibilité, d'intégrité ou de confidentialité de ces actifs sur l'organisme et sa clientèle ou sur d'autres organismes.

- **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 tels que les fournisseurs, etc.

5. MODALITÉS

5.1 Énoncés et principes généraux

Le dirigeant d'organisme (DO), qui est le président-directeur général du CIUSSS de la Capitale-Nationale, 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. Il concrétise cette volonté par une gouverne forte, évolutive et adaptée de la sécurité de l'information qui permet d'instaurer une saine culture organisationnelle en la matière.

5.2 Développement d'une saine culture en sécurité de l'information

5.2.1. Le développement d'une telle culture dans l'organisation tient compte :

- Des aspects humains, organisationnels, financiers, juridiques et technologiques;
- De sa mission et de ses lignes d'affaires;
- De l'environnement technologique perpétuellement en changement et interconnecté avec le monde;
- De la pérennité de l'expertise en sécurité de l'information, notamment grâce à la formation continue, le soutien nécessaire ainsi qu'à l'attraction et à la rétention des ressources humaines.

5.2.2 Le CIUSSS de la Capitale-Nationale 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. En favorisant et encourageant des actions d'éducation, l'organisation promeut l'adoption de comportements sécuritaires quant aux cybermenaces.

5.2.3 Le renforcement des dispositifs de prévention et de réaction à l'égard des cybermenaces, dans une perspective de protection de l'information et de résilience des actifs informationnels, implique d'aller au-delà des réalisations en silo et de prôner une ouverture sur le partage et la mise en commun des connaissances, de l'expertise et des bonnes pratiques en cybersécurité avec le Réseau et les partenaires stratégiques du Gouvernement du Québec.

5.3 Imputabilité

5.3.1. La sécurité de l'information représente une responsabilité collective où chaque utilisateur est imputable de l'utilisation qu'il fait de l'information dont il a été dûment autorisé à avoir accès. À cette fin, l'utilisateur répond de ses actions auprès du DO.

5.3.2. Le CIUSSS de la Capitale-Nationale 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.

5.3.3. Tout manquement à la sécurité de l'information fait l'objet d'une vérification et l'application de mesures correctrices peut être exigée.

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 représente un sous-ensemble de la gestion globale des risques de l'organisation et qui s'y intègre harmonieusement, en mode amélioration continue.
- Fournit une lecture des risques qui favorise la mise en place de mesures de sécurité de l'information proportionnelles à la valeur de l'information et aux risques encourus, réduisant ainsi ces risques de façon efficace.
- Implique que la gestion de la désuétude technologique guide les choix de l'organisation en matière de ressources informationnelles. L'exploitation des vulnérabilités technologiques étant un des plus grands risques de sécurité.

5.4.2. Le chef de la sécurité de l'information organisationnelle (CSIO) évalue sur une base régulière et dans le cadre de projets d'informatisation ou d'acquisition d'application infonuagique, les risques d'atteinte à la disponibilité, l'intégrité et la confidentialité de l'information et s'assure de la mise en place de mesures d'atténuation des risques. La protection de l'information en amont permet d'être proactif à l'égard des cybermenaces émergentes et de minimiser les risques.

5.5 Protection des renseignements personnels à toutes les étapes du cycle de vie d'un actif informationnel

5.5.1. La gestion de la sécurité demande la mise en place d'un ensemble de processus de travail supportant les besoins d'affaires et basé sur une bonne connaissance des cybermenaces afin de protéger en tout temps les renseignements personnels. La mise en place de mesures en matière de cybersécurité s'appuie sur la catégorisation et la classification de l'information en fonction de sa sensibilité.

5.5.2. La gestion des événements de sécurité :

- Est réalisée dans une dynamique de travail collaboratif qui implique l'ensemble des intervenants, permettant la canalisation et la mutualisation des efforts afin de corriger les situations qui exigent une intervention;
- Met de l'avant une prise en charge rapide, de sa détection jusqu'à sa résolution;
- N'est pas improvisée et s'appuie sur un processus clair et agile afin de traiter promptement les situations qui nécessitent une escalade à un niveau supérieur. Des instances de coordination et de concertation sont en place, notamment afin d'assurer des communications fluides entre les intervenants.

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 provincial de gestion de la sécurité de l'information (MSSS-CDG01) et transposé et adapté dans le Cadre de gestion de la sécurité de l'information du CIUSSS de la Capitale-Nationale. Ce cadre définit les responsabilités des intervenants en matière de sécurité informationnelle soit :

- Le conseil d'administration
- Le dirigeant d'organisme (DO)
- Le chef de la sécurité de l'information organisationnelle (CSIO)

- Le coordonnateur organisationnel des mesures de sécurité de l'information (COMSI)
- Les détenteurs de l'information
- Les gestionnaires
- Les utilisateurs

7. ENTRÉE EN VIGUEUR

La présente politique entre en vigueur le jour suivant son adoption par le conseil d'administration.

8. ANNEXES

Annexe 1 : Cadre légal et administratif

ANNEXE 1

Cadre légal et administratif

La présente politique s'inscrit principalement dans un contexte régi par :

- La Loi modifiant la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LQ 2021, chapitre 22);
- 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;
- Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, LQ 2021, c. 25;
- Loi sur les renseignements de santé et de services sociaux et modifiant diverses dispositions législatives, 2023, c. 5;
- 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 les coroners, chapitre, C-68.01;
- Le Code des professions, L.R.Q., c. C-26, articles 60.4 et 60.6 et 87;
- Code de déontologie des membres de l'Ordre professionnel des travailleurs sociaux et des thérapeutes conjugaux et familiaux du Québec, C-26, r.28;
- 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 directive gouvernementale sur la sécurité de l'information, décret 1514-2021.