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

Québec

POLITIQUE

PO-18-001	**Politique de sécurité de l'information**	
Direction responsable : Direction des ressources technologiques et informationnelles		**Entrée en vigueur : 2017-09-27**
☒ **Politique organisationnelle** ☐ **Politique spécifique**		**Révisée le : 2020-01-21**
Destinataires : Tous les membres du personnel, les médecins, les stagiaires, les bénévoles, les mandataires et les fournisseurs de l'organisation		
Document(s) associé(s) :		

1. PRÉAMBULE

Les services offerts à la population par le CIUSSS du Nord-de-l'Île-de-Montréal (CIUSSS NIM) reposent en grande partie sur l'information recueillie, produite, utilisée et communiquée. Ces informations sont variées et exigent de plus en plus le recours aux technologies. Certaines de ces informations présentent un haut degré de sensibilité parmi lesquelles figurent des renseignements personnels portant sur des usagers, des médecins, des membres du personnel ou des stagiaires.

Comme toute organisation du réseau de la santé et des services sociaux, il appartient au CIUSSS NIM de protéger ces informations de manière adéquate au regard des exigences légales, réglementaires ou contractuelles, tout en tenant compte des menaces possibles auxquelles il doit faire face.

Conscient de l'importance de ces informations et de sa responsabilité, la direction du CIUSSS NIM exprime, par le biais de cette politique, sa volonté de mettre en place toutes les mesures de sécurité appropriées.

2. OBJECTIFS

Cette politique témoigne de l'engagement de la haute direction du CIUSSS NIM envers la sécurité de l'information. Elle constitue le premier niveau du cadre normatif visant à :

- sécuriser l'information tout au long de son cycle de vie;
- assurer la protection de l'information confidentielle contre les accès non autorisés;
- assurer la qualité de l'information et la protéger contre toute atteinte à son intégrité et à sa disponibilité;
- assurer, lorsque nécessaire, l'irrévocabilité des documents et l'authentification de leur auteur.

3. DÉFINITIONS

Actif informationnel

Au sens de la Loi, un actif informationnel réfère au partage de certains renseignements de santé, soit par le biais d'une banque d'information, d'un système d'information, d'un réseau de télécommunication, d'une infrastructure technologique ou d'un ensemble de ces éléments. L'actif informationnel implique aussi une composante informatique d'un équipement médical spécialisé ou ultraspécialisé. Est également considéré comme un actif informationnel tout support papier contenant de l'information.

Détenteur

Un gestionnaire (cadre) du CIUSSS NIM 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.

Utilisateur

Toute personne du CIUSSS NIM de quelque catégorie d'emploi, de statut d'employé ainsi que toute personne morale ou physique qui, par engagement contractuel ou autrement, utilise un actif informationnel sous la responsabilité de l'organisme ou elle y a accès.

Disponibilité

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

Intégrité

Propriété d'une information qui ne subit aucune altération ou destruction de façon erronée ou sans autorisation et qui est conservée sur un support lui procurant stabilité et pérennité. L'intégrité fait référence à l'exactitude et à la complétude.

Confidentialité

Propriété d'une information qui n'est accessible ou divulguée qu'aux personnes ou entités désignées et autorisées.

Cycle de vie de l'information

L'ensemble des étapes que franchi 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 du CIUSSS NIM.

Risque de sécurité de l'information

Probabilité que survienne un événement préjudiciable, plus ou moins prévisible, qui peut affecter la réalisation des objectifs du CIUSSS NIM.

Incident affectant l'information

Conséquence observable de la concrétisation d'un risque à la sécurité de l'information.

4. CHAMP D'APPLICATION

Cette politique porte sur l'information détenue ou utilisée par le CIUSSS NIM, peu importe sa nature, son emplacement ou le support sur lequel elle se trouve et ce, tout au long de son cycle de vie. Elle concerne également l'information confiée à des tiers.

Cette politique doit être considérée en tout temps, notamment dès l'étape de conception d'un processus ou d'un système d'information, ou lors de l'élaboration d'ententes ou l'acquisition d'une solution technologique.

Cette politique s'applique à tout le personnel du CIUSSS NIM, les employés, les gestionnaires, les médecins, les résidents en médecine, les chercheurs, les étudiants, les bénévoles, les mandataires, les fournisseurs ainsi qu'à ceux qui interviennent pour leur compte. Elle s'applique également à tout détenteur d'un actif informationnel du CIUSSS NIM.

5. PRINCIPES DIRECTEURS

5.1 Cadre de références (SEC-P1)

La présente politique s'appuie sur la norme internationale ISO-27000 : Normes de sécurité de l'information, qui propose les meilleures pratiques en cette matière.

5.2 Responsabilisation et sensibilisation des utilisateurs (SEC-P2)

Chaque personne ayant accès aux actifs informationnels contribue activement à la sécurité et l'intégrité de ceux-ci. Elle est sensibilisée aux risques et reçoit les formations appropriées aux fonctions qu'elle occupe. Elle reconnait qu'elle peut avoir sous sa responsabilité des données de nature confidentielle, notamment des renseignements personnels. Par conséquent, elle doit prendre les mesures de sécurité propres à assurer la protection des renseignements collectés, utilisés, communiqués, conservés ou détruits.

5.3 Gestion de l'information (SEC-P3)

Tout actif informationnel fait l'objet d'une identification et le niveau d'exigence de sécurité le concernant est établi par son détenteur qui doit être identifié. Tout actif informationnel doit être assigné à un propriétaire.

5.4 Gestion des risques et conformité (SEC-P4)

Sous réserve d'obligations légales, réglementaires ou contractuelles, le choix des mesures de sécurité est fait en tenant compte, non seulement du niveau d'exigence de sécurité établi par son détenteur, mais également des menaces et des risques auxquels l'actif est exposé. Ces risques sont réévalués périodiquement afin de s'assurer que les mesures en place sont toujours appropriées. Le cadre légal comprend de manière non exhaustive :

- la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, c. M-19.2, a. 5.2);
- la Loi sur le Ministère de la Santé et des Services sociaux (RLRQ, c. M-19.2, a. 5.2);
- la Loi concernant le partage de certains renseignements de santé (RLRQ, c. P-90001, a. 4 et 5);
- la Loi sur la santé et les services sociaux (RLRQ, c. S-4.2) détermine le rôle d'un établissement de santé et traite également de la sécurité des actifs informationnels (AI).

5.5 Gestion des identités et des accès (SEC-P5)

L'accès aux actifs informationnels est contrôlé de manière à s'assurer qu'il soit limité aux seules personnes autorisées, et ce, dans la mesure où cet accès est nécessaire pour l'accomplissement de leurs tâches, tout en veillant à la séparation des tâches incompatibles.

5.6 Sécurité des systèmes d'information et de leur environnement (SEC-P6)

Les systèmes d'information et l'environnement dans lequel ils se trouvent sont sécurisés de manière à répondre aux exigences de sécurité de l'information prise en charge. Des outils sont mis en place pour assurer l'actualisation des accès et opérations liés aux actifs de l'information si un cadre légal ou normatif s'applique.

5.7 Gestion des incidents (SEC-P7)

Un processus de gestion des incidents affectant l'information est élaboré et mis en place afin de permettre une réaction appropriée et de limiter les conséquences sur les personnes et les services. Cette gestion des incidents est prise en compte lors des activités d'amélioration continue des façons de faire et des mesures de sécurité.

5.8 Vérification, audits et enquêtes (SEC-P8)

Être à même d'effectuer des vérifications ciblées ou encore des enquêtes informatiques lorsque des activités contreviennent aux législations, aux politiques, aux règlements, aux conventions et aux ententes du CIUSSS NIM. Ce type d'interventions doit cependant être encadré par un processus rigoureux impliquant des personnes dûment habilitées à les réaliser.

5.9 Plan de continuité (SEC-P9)

Se prémunir contre les interruptions de service prolongées en disposant d'un plan de continuité permettant d'assurer la remise en opération des services jugés essentiels en cas de sinistre majeur.

6. MODALITÉS

6.1 Mesures d'exception

Toute exception à l'application d'une exigence de sécurité, dont la demande doit être effectuée dans le cadre d'un processus établi comportant une évaluation préalable des risques associés à cette exception. Toute exception est obligatoirement limitée dans le temps et les risques doivent être quantifiés via une analyse de risques et acceptés par le propriétaire des données.

6.2 Droits de regard et sanctions

Le CIUSSS NIM a un droit de regard sur l'utilisation de ses actifs informationnels. Les membres du personnel qui ne respectent pas la politique s'exposent à des mesures administratives ou des sanctions disciplinaires. Les partenaires, les mandataires et les fournisseurs sont passibles de mesures administratives telles que la résiliation du contrat ou l'expulsion de la personne qui travaille pour leur compte. De surcroît, des poursuites pénales pourront être engagées contre toute personne fautive.

7. RÔLES ET RESPONSABILITÉS

7.1 Conseil d'administration

Le CA approuve la présente politique ainsi que ses mises à jour.

7.2 Président-directeur général (PDG)

Le PDG est le premier responsable de la sécurité de l'information. Il nomme le responsable de la sécurité de l'information.

7.3 Le responsable de la sécurité de l'information (RSI)

Le RSI veille, pour le PDG au respect de la présente politique. Il gère et coordonne la sécurité de l'information au sein de l'organisation.

7.4 Le comité de direction

Le comité de direction doit :

- s'assurer de l'application de la politique par les gestionnaires du CIUSSS NIM;
- s'assurer que le RSI dispose des ressources financières et logistiques appropriées.

7.5 Les directions et services

Chaque direction est imputable de la gestion des risques liés à l'utilisation de l'information sous sa responsabilité. Cette imputabilité s'applique à tous les actifs informationnels (papiers, processus et systèmes) qu'elle utilise. Elle doit notamment :

- nommer un détenteur d'actif informationnel pour chaque actif à protéger;
- informer le RSI de tout risque important à la sécurité de l'information;
- s'assurer de l'application de la présente politique dans sa direction.

7.6 La direction des ressources informationnelles

La direction des ressources informationnelles assiste les directions dans l'évaluation et la gestion des risques à la sécurité. Elle doit notamment :

- maintenir la liste des détenteurs d'actifs informationnels propriétaires des systèmes d'information;
- effectuer des évaluations de risque périodiques ou au besoin et communiquer les résultats au RSI; déployer des mesures de sécurité appropriées et approuvées par le propriétaire de l'information;
- appuyer le RSI dans la mise en œuvre du programme de sensibilisation à la sécurité de l'information pour les membres du personnel;
- mettre en œuvre les directives, processus et standards touchant à la sécurité des actifs informationnels, touchant notamment la gestion des accès, la gestion des incidents et l'intégrité de l'information.

7.7 L'officier de sécurité

Il est nommé par le responsable de la sécurité de l'information. Il est autorisé à effectuer des enquêtes, audits et analyses de sécurité physique ou logique dans le cadre d'une procédure rigoureuse et prédéterminée.

7.8 Les détenteurs d'actifs informationnels

Tout détenteur est responsable d'établir le niveau d'exigence de sécurité attendu pour l'actif qui lui a été confié et d'assurer la gestion des risques le concernant.

Tout détenteur est responsable d'établir le niveau d'exigence de sécurité attendu pour l'actif qui lui a été confié et d'assurer la gestion des risques le concernant. Des mesures raisonnables, basées sur les niveaux de risques doivent être mises en place pour protéger ces actifs. Il agit en tant que responsable désigné par sa direction en appliquant les dispositions suivantes issues de la présente politique :

- effectue la classification de sécurité de l'information et communique les résultats au conseiller à la sécurité de l'information;
- établit et révise périodiquement en fonction des cadres légaux et standards, les profils d'accès des utilisateurs et les communique aux intervenants pertinents;
- identifie les exigences légales, réglementaires et contractuelles applicables à la sécurité de l'information en collaboration avec le service des affaires juridiques et le conseiller à la sécurité de l'information;
- effectue l'évaluation des risques à la sécurité de l'information avec l'aide du conseiller à la sécurité de l'information et lui en communique les résultats;
- accepte, au nom de son unité administrative, les risques résiduels à la sécurité de l'information;
- nomme les directions et ressources responsables d'appliquer ces mesures et en garantit le suivi et la bonne application.

7.9 Les gestionnaires

Tout gestionnaire est responsable de l'application et du respect de cette politique au sein de son secteur d'activité. Il sensibilise son personnel à la sécurité de l'information, aux conséquences d'un manquement à la présente politique et à la responsabilité de chacun en la matière.

7.10 Les utilisateurs

Tout utilisateur a l'obligation de protéger l'information mise à sa disposition. Il est notamment responsable de :

- respecter les directives et les consignes qui lui sont communiquées;
- utiliser l'information avec discernement, aux seules fins pour lesquelles elle est destinée et selon les droits qui lui sont accordés;
- agir avec précaution;
- respecter les droits de propriété intellectuelle;
- signaler immédiatement à son supérieur toute situation pouvant compromettre la sécurité de l'information;
- utiliser les actifs informationnels en se limitant aux fins pour lesquelles ils sont destinés et à l'intérieur des accès qui lui sont accordés.

8. BIBLIOGRAPHIE

MSSS-POL01 Politique provinciale de la sécurité de l'information - 2015-08-17

9. PRÉCISIONS

ÉLABORATION :	Direction des Ressources Technologiques et Informationnelles
COLLABORATION :	Toutes les directions
ANNULE ET REMPLACE :	
ADOPTÉ PAR : **DATE** : **NO. RÉSOLUTION**	Conseil d'administration CIUSSS du Nord-de-l'Île-de-Montréal 2020-01-21 2019-12/1061
RÉVISION (année) :	2023