Centre intégré de santé et de services sociaux de la Côte-Nord
Québec

# POLITIQUE

## Sécurité de l'information

Numéro G1-252-004

**Direction des ressources informationnelles**

## 1. PRÉAMBULE

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 de santé et de services sociaux de la Côte-Nord, ci-après appelé l'établissement, 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. CONTEXTE LÉGAL ET ADMINISTRATIF

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, 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. BUT

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.

## 4. OBJECTIFS

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 sert de fondation en matière de sécurité de l'information dans l'établissement. Elle permet également au responsable de la sécurité de l'information de définir un ensemble de principes visant à :

4.1 Assurer la disponibilité, l'intégrité et la confidentialité de l'information 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.

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

4.3 Protéger les informations des usagers.

4.4 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.

4.5 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.

## 5. CHAMP 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 tout utilisateur 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.

## 6. 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'organisme.

**Détenteur de l'information** : Un employé désigné par son établissement, 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. Le terme « détenteur de processus d'affaires » est utilisé lorsque ce rôle se limite à un processus d'affaires déterminé.

**Pilote de système d'information :** Personne, nommée par le détenteur de système, qui agit comme intermédiaire entre l'équipe de développement informatique et les utilisateurs de système. Le pilote de système est en quelque sorte le superutilisateur. Il est responsable d'appliquer les configurations avancées dans le système, il est la personne de référence pour les utilisateurs lorsqu'ils ont des problèmes ou questions avec le système. Cette personne est aussi responsable de faire des essais utilisateurs avant les mises en production du système.

**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 autorisations 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.

**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.

**Utilisateur :** Toute personne de l'établissement de quelques catégories d'emplois, 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'établissement ou y a accès.

## 7. RESPECT DE LA POLITIQUE

L'établissement oblige tous les utilisateurs à la signature d'un engagement à la confidentialité et au respect des politiques et documents d'encadrement.

## 8. 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.

Tout utilisateur 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 autorisations;
- 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 autorisations.

## 9. ROLES, RESPONSABILITES ET IMPUTABILITÉ

La présente politique de sécurité fixe les obligations en matière de sécurité de l'information attribuées au président-directeur général, au responsable de la sécurité de l'information, aux gestionnaires et aux utilisateurs.

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 établissement. 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.

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

Les détenteurs de l'information sont responsables d'assurer la sécurité d'un ou de plusieurs actifs informationnels qui leur sont confiés et des ressources qui les sous-tendent.

Les gestionnaires sont chargés de la mise en œuvre des dispositions de la présente politique auprès du personnel relevant de leur autorité.

Tout utilisateur doit se conformer à la présente politique, au cadre de gestion et tout autre document d'encadrement qui appuie la politique. Il doit veiller à la protection des actifs informationnels mis à sa disposition, en se limitant aux fins auxquelles ils sont destinés et répond de ses actions auprès du président-directeur général de l'établissement. Il avise, également, son supérieur immédiat de toute situation portée à sa connaissance et qui est susceptible de compromettre la sécurité de l'information de son établissement.

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

## 10. DROIT DE REGARD

Le président-directeur général ou le responsable des actifs informationnels 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*.

## 11. SANCTIONS

Lorsqu'un utilisateur ou une organisation contrevient ou déroge à la présente politique ou aux directives et procédures et tous 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.

## 12. 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.

## 13. HISTORIQUE DES VERSIONS

| | | Préparée par | Instances consultées | | | | | | | Entrée en vigueur |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | CODIR | CII | CM | CMDP | Comité de sécurité | | Autres | |
| Versions | 1 | **Anna Dionne**, chargée de projets DRI<br>**Anne Paquet**, conseillère en gouvernance de la sécurité de l'information<br>**François Otis**, chef de service exploitation et infrastructure<br>**Michel Rioux**, directeur ressources informationnelles | x | | | | x | | | Le 10 février 2016 |
| | 2 | | | | | | | | | |

*Légende*

| | | | |
|---|---|---|---|
| *CODIR* | *Comité de direction* | *CM* | *Conseil multidisciplinaire* |
| *CII* | *Conseil des infirmières et infirmiers* | *CMDP* | *Conseil des médecins, dentistes et pharmaciens* |

## APPROPRIATION ET IMPLANTATION

| DOCUMENT | | APPROPRIATION | | | |
|---|---|---|---|---|---|
| | **CIBLE** | **COTE** | **RESPONSABLE** | **MOYENS** | **DATE** |
| Politique – Sécurité de l'information | Directeurs | M | DRI | Comité de direction | 2016-xx-xx |
| | Cadres intermédiaires | M | Directeurs | Rencontre d'équipe | 2016-xx-xx |
| | Employés | M | DRI | Note de service et séances d'information | 2016-xx-xx |
| | | | Cadres intermédiaires | Rencontres d'équipe | 2016-xx-xx |
| | | | DRH | Information et signature du formulaire | À l'embauche |
| | Médecins, résidents, organismes partenaires, bénévoles, stagiaires, contractuels, fournisseurs de services | M | Gestionnaires concernés | Rencontres | 2016-xx-xx, aux besoins et annuellement |
| | | **IMPLANTATION** | | | |
| | | | Directeur<br>Gestionnaires<br>Employés | Rencontre d'équipe<br>Rencontre d'équipe<br>Consultation du document | 2016 et annuellement |

M – À maitriser C – À connaître I – Être informé

| Catégorie | Critères de sélection |
|---|---|
| À maitriser | • Impact direct sur la pratique<br>• Influence directe dans la qualité de la prestation de services<br>• En réponse directe aux besoins de la clientèle<br>• Assure le respect des droits de l'usager<br>• Application du document de façon régulière |
| À connaître | • Doit posséder les compétences requises pour la mettre en application<br>• Aide à la compréhension des actions des collaborateurs<br>• Peut orienter une décision, une intervention<br>• Applique le document de façon occasionnelle |
| Être informé | • Doit savoir que ce document existe afin de respecter les orientations et les normes de l'établissement<br>• Touche de loin ou indirectement la pratique auprès de l'usager<br>• N'est pas d'une utilité immédiate<br>• Applique la politique rarement ou exceptionnellement |

## 14. RÉFÉRENCES

*Politique provinciale sur la sécurité de l'information,* ministère de la Santé et des Services sociaux, août 2015.

*Politique de sécurité des actifs informationnels*, Agence de la santé et des services sociaux de la Côte-Nord, juin 2005.

Centre intégré
de santé
et de services sociaux
de la Côte-Nord
Québec

# Formulaire d'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 de sécurité de l'information du Centre intégré de santé et de services sociaux de la Côte-Nord.

**Je m'engage** à prendre connaissance, respecter cette politique et à appliquer ses lignes de conduite dans le but de préserver la sécurité de l'information 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 Centre intégré de santé et de services sociaux de la Côte-Nord exerce une surveillance des systèmes d'information. J'ai également été informé(e) que les systèmes d'information 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, comme stipulé dans la Politique de sécurité de l'information, peuvent entraîner 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, comme stipulé dans le code d'éthique de l'établissement, 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 Centre intégré de santé et de services sociaux de la Côte-Nord.**

*Cocher la case appropriée*

☐ Employé ☐ Médecin ☐ Résident ☐ Stagiaire ☐ Étudiant
☐ Recherche ☐ Bénévole ☐ Contractuel ☐ Fournisseur

| Nom et prénom (lettres carrées) | Numéro employé | Numéro pratique |
|---|---|---|
| | | |

Signature de la personne

Signature du représentant de l'établissement

Original au dossier de la personne