CHU Sainte-Justine
Le centre hospitalier universitaire mère-enfant

Pour l'amour des enfants

Université de Montréal

POLITIQUES ET PROCÉDURES ADMINISTRATIVES
CHU SAINTE-JUSTINE

Titre : POLITIQUE SUR LA SÉCURITÉ DE L'INFORMATION Sécurité des actifs informationnels	**Codification : POL-243** **Niveau d'application :** Général
Responsable : Rémi Forget Direction Qualité Performance **Signature :** 	**Approuvé par :** Comité de direction **En vigueur le** : 1 Juin 2018 **Révisé le :** 1 Juin 2018

1.0 CONTEXTE

Le CHU Sainte-Justine applique depuis septembre 2002, le cadre global de gestion des actifs informationnels – volet sécurité(CGGAI) du Ministère de la santé et des services sociaux. Celui-ci décrit un ensemble d'énoncés et de principes, les rôles et responsabilités ainsi que les mesures de sécurité que les organismes du Réseau de la santé et des services sociaux (RSSS) doivent respecter et mettre en œuvre.

La mise en œuvre du CGGAI a permis d'introduire une culture de sécurité de l'information au CHU Sainte-Justine et d'améliorer le niveau global de sécurité des actifs informationnels. Toutefois, l'évolution des pratiques, la modernisation des services et les nouvelles exigences du Secrétariat du Conseil du trésor (SCT) en matière de sécurité de l'information augmentent les besoins d'échanges d'information et de mobilité des intervenants en santé et services sociaux. Ces nouveaux besoins rendent nécessaire l'évolution de l'encadrement de la sécurité de l'information.

Pour se donner les conditions permettant de relever ces défis et considérant l'apport grandissant des technologies de l'information à l'innovation, à la dispensation des soins et à la transformation de la pratique clinique, le CHU Sainte-Justine reconnaît la nécessité d'assurer la disponibilité, l'intégrité et la confidentialité de l'information. Pour ce faire, il met en place une gouverne claire de la sécurité de l'information, dont la présente politique constitue l'élément de base.

Plusieurs lois, règlements, directives ou politiques encadrent et régissent l'utilisation et la gestion de l'information. Le CHU Sainte-Justine doit s'assurer de respecter ce cadre normatif.

2.0 OBJECTIFS

La présente politique vise à assurer le respect du cadre normatif relatif à la sécurité de l'information et à l'utilisation des technologies de l'information et des télécommunications.

Plus spécifiquement, les objectifs du CHU Sainte-Justine en matière de sécurité de l'information sont d'assurer :

2.1 Le respect de la vie privée des individus, notamment, la confidentialité des renseignements personnels relatifs aux patients, aux participants à des études de recherche et aux intervenants du Réseau de la santé et des services sociaux.

2.2 La disponibilité, l'intégrité et la confidentialité de l'information à l'égard de l'utilisation qui en est faite au CHU Sainte-Justine.

2.3 Le respect des mesures de sécurité concernant l'utilisation des actifs informationnels.

2.4 La conformité aux lois et règlements applicables ainsi qu'aux directives, normes et orientations gouvernementales.

Cette politique sera suivie d'un cadre de gestion local de la sécurité de l'information, d'un système de gestion de la sécurité de l'information, et d'un cadre normatif en sécurité de l'information qui inclura des Politiques, processus et des registre.

3.0 RESPECT DE LA POLITIQUE

Le président directeur général du CHU Sainte-Justine désigne le responsable de la sécurité de l'information (RSI) comme responsable de l'application de la présente politique.

Le CHU Sainte-Justine exige de toute personne qui utilise ses actifs informationnels, qu'elle se conforme aux dispositions de la présente politique ainsi qu'aux mesures, directives et procédures qui s'y rattachent.

4.0 PORTÉE

La présente politique s'applique aux personnes suivantes:

- Tous les intervenants du CHU Sainte-Justine.
- Toute personne physique ou morale dûment autorisée à avoir accès et à utiliser les actifs informationnels détenus par le CHU Sainte-Justine.

La présente politique régit :

- L'ensemble des contrats ou ententes de service liant le CHU Sainte-Justine avec ses fournisseurs et partenaires. Ces contrats et ententes doivent contenir les dispositions requises pour garantir le respect de la présente politique, de la Règle particulière en sécurité de l'information et des autres règles qui en découlent.
- L'ensemble des activités de création, de collecte, de stockage, d'analyse, de transfert, de consultation et de communication de l'information.

5.0 PRINCIPES DIRECTEURS

5.1 Le CHU Sainte-Justine reconnaît que la gouvernance de la sécurité de l'information est basée sur une prise en charge engagée mettant en avant-plan l'amélioration continue, la proactivité et la reddition de comptes à tous les niveaux hiérarchiques et ce au sein de toutes les directions, tout en favorisant une collaboration soutenue entre les différents intervenants.

5.2 Le président directeur général du CHU Sainte-Justine 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.

5.3 Toute personne autorisée à avoir accès aux actifs informationnels du CHU Sainte-Justine assume les responsabilités que lui confère la présente politique en matière de sécurité de l'information, et répond de ses actions auprès du président directeur général de l'établissement.

5.4 La mise en œuvre de la politique tient compte des aspects humains, éthiques, déontologiques, organisationnels, financiers, juridiques et techniques, et requiert, à cet égard, la mise en place d'un ensemble de mesures coordonnées.

5.5 Les mesures de surveillance de l'utilisation des actifs informationnels doivent permettre d'assurer la disponibilité, l'intégrité, la confidentialité de ceux-ci, de même que la continuité des activités. Ces mesures doivent notamment permettent de prévenir les accidents, la malveillance ou la destruction non autorisée d'informations.

5.6 Les principes de la présente politique doivent être appliqués tout au long du processus menant à l'acquisition, au développement, à l'utilisation, à l'entretien, au remplacement ou la destruction d'un actif informationnel par ou pour le CHU Sainte-Justine.

5.7 Les ententes et contrats ayant pour objet l'acquisition, le développement, l'utilisation, l'entretien, le remplacement ou la destruction d'un actif informationnel du CHU Sainte-Justine doivent contenir des dispositions garantissant le respect des exigences en matière de sécurité de l'information, tel que décrit dans la règle particulière en sécurité de l'information.

6.0 GESTION INTÉGRÉE DES RISQUES RELIÉS À LA SÉCURITÉ DE L'INFORMATION

6.1 La gestion intégrée des risques reliée à la 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 reliés à la sécurité de l'information à tous les niveaux hiérarchiques, au sein de toutes les directions.

6.2 Les risques d'atteinte à la disponibilité, l'intégrité ou la confidentialité de l'information, pouvant affecter la réalisation des missions de l'établissement, doivent être évalués régulièrement. Des mesures permettant de réduire ces risques doivent être mises en place.

6.3 Le CHU Sainte-Justine doit mettre en œuvre des processus de gestion des risques reliés à la sécurité de l'information. Tout manquement aux règles de sécurité de l'information doit faire l'objet d'une analyse appropriée afin de rendre compte de la situation au Responsable de la sécurité de l'information du CHU Sainte-Justine.

7.0 RÔLES ET RESPONSABILITÉS

Le responsable de la sécurité de l'information (RSI), délégué par le président directeur général du CHU Sainte-Justine, est responsable de l'application de la présente politique.

La structure fonctionnelle de la sécurité de l'information du CHU Sainte-Justine ainsi que les rôles et responsabilités des principaux intervenants en sécurité de l'information sont définis dans le cadre de gestion local de la sécurité de l'information (CGSI) qui vient compléter les dispositions de la présente politique.

8.0 SENSIBILISATION ET FORMATION

8.1 Le CHU Sainte-Justine doit dispenser à ses intervenants, sur une base régulière, des activités de sensibilisation et de formation, afin que ceux-ci disposent des connaissances nécessaires pour assurer la sécurité de l'information, en fonction de leurs rôles et responsabilités.

8.2 Les intervenants en sécurité de l'information doivent recevoir une formation et le soutien nécessaire pour s'assurer qu'ils maîtrisent les concepts requis pour leur permettre d'exercer leur rôle.

9.0 GESTION DES IDENTITÉS, DES ACCÈS ET DES BIENS CONFIÉS

Le CHU Sainte-Justine est muni d'un système de gestion des identités, des accès et des biens confiés (GIA), dont le but est de s'assurer que les bons intervenants ont les bons accès et ce au bon moment. Pour que la gestion des identités, des accès et des biens confiés soit efficace et faite de façon sécuritaire, les sources RH autoritaires et les applications doivent être interfacées avec le système de GIA. Ce système permet notamment :

- Une meilleure sécurité informationnelle via contrôle de l'identité et des accès numériques des intervenants
- Une visibilité centralisée sur les accès des intervenants
- L'amélioration et l'optimisation des processus liées à la gestion des accès
- Une réduction des délais de traitement et du temps investi dans la création, la modification et la révocion des droits d'accès;

10.0 SANCTIONS

Le non-respect des obligations prévues à la présente politique et dans politique sur l'utilisation acceptable des technologies de l'information (POL-241) peut entraîner des mesures disciplinaires ou administratives selon le cas.

11.0 DISPOSITIONS FINALES

La présente politique entre en application au moment où elle sera adoptée par le conseil d'administration. Cette politique est réévaluée minimalement aux trois ans afin de tenir compte des nouveaux besoins, des nouvelles pratiques, des nouvelles menaces et des nouveaux risques encourus.

12.0 DÉFINITIONS

Terme	Description
Actif informationnel	Toute information détenue par le CHUSJ, que son support fasse appel ou non aux technologies de l'information, ainsi que, tel que défini dans la Loi concernant le partage de certains renseignements de santé, RLRQ chapitre P-9.0001, toute banque d'information, tout système d'information, réseau de télécommunication, infrastructure technologique ou un ensemble de ces éléments ainsi qu'une composante informatique d'un équipement médical spécialisé ou ultra spécialisé.
Actif physique	L'ensemble des ressources matérielles non technologiques, notamment les bâtiments, les locaux, les systèmes de prévention d'incendie, les classeurs, etc.
Analyse du risque	Étude qui permet de déterminer le degré de risque et d'évaluer les conséquences directes et indirectes, tangibles et intangibles d'un événement sur une organisation et son environnement. [i]
Atelier de catégorisation	Rencontre entre les différents intervenants afin de classifier un système d'information.
Catégorisation d'un système d'information	Attribuer un niveau d'importance aux propriétés de sécurité d'un système d'information. L'attribution doit tenir compte des exigences légales, de la sensibilité et du caractère critique du système pour HEC Montréal.
Confidentialité	Caractère des données dont la diffusion doit être limitée aux seules personnes ou autres entités autorisées. [i]
Disponibilité	Assurer que l'information est disponible au moment où elle est requise.
Dysfonctionnement	Événement qui affecte des opérations et/ou des données et ayant un impact sur une ou des propriétés de sécurités.
Impact	Conséquence, effet d'un événement affectant les objectifs.
Information	Renseignement consigné sur un support quelconque (papier ou électronique) ou communiqué dans un but de transmission des connaissances. À titre d'exemple, l'information comprend les fichiers structurés (bases de données) et non structurés (fichiers Word, Excel, PowerPoint, PDF, etc.), les courriels, les messages texte, les communications et les messages vocaux, photos, dessins, télécopies, originaux et copies de documents papier, rapports informatisés ainsi que les copies de sauvegarde et les archives. [iii]
Intégrité	Propriété associée aux données, peu importe le support (papier, document électronique, base de données, CD-ROM, etc.), qui, lors de leur traitement ou de leur transmission, ne subissent aucune altération ou destruction volontaire ou accidentelle, et conservent un format permettant leur utilisation. [i]
Intervenant	Ensemble des individus œuvrant au CHU Sainte-Justine (médecins, dentistes, pharmaciens, autres professionnels de la santé, chercheurs, employés, travailleurs autonomes, résidents, stagiaires et étudiants, incluant les employés du CHUSJ exerçant leur profession au sein d'entités externes telles des écoles ou l'équipe santé enfance jeunesse).
Logiciel	Ensemble des ressources issues de la programmation destiné à effectuer un traitement particulier sur un ordinateur, notamment les systèmes d'exploitation, les progiciels, les applications bureautiques, etc. [i]

Matériel technologique	Ensemble des ressources matérielles de nature technologique, notamment les ordinateurs de table, les ordinateurs portables, les écrans, les tablettes, les téléphones, les imprimantes, etc. [i]
Plausibilité	Possibilité que quelque chose se produit.
Procédure	Une procédure est une série de tâches reliées entre elles et formant une séquence préalablement définie qu'il faut accomplir pour produire un résultat; elle précise le quoi, le comment, le quand et les intervenants. Les procédures sont des plans qui définissent les méthodes qui devront être utilisées dans l'exécution des activités prévues. Elles guident davantage l'action que la réflexion et expliquent en détail et de façon précise, la manière d'accomplir une certaine activité. Essentiellement, elles se distinguent par la séquence chronologique de leur contenu. La procédure doit être précise et ne laisser aucune place à l'interprétation.
Processus	Ensemble d'activitéslogiquement interreliées qui produisent un résultat déterminé. [i]
Propriété de sécurité	Les propriétés de sécurité sont la disponibilité, l'intégrité et la confidentialité. Ces propriétés sont associées à un système d'information et un niveau d'importance pour chacune d'elles est déterminé.
Ressource informationnelle	Ensemble de tous les éléments faisant partie d'un ou de plusieurs systèmes d'information du CHU Sainte-Justine impliqué dans le traitement, le stockage ou la communication de l'information.
Risque inhérent	Évaluation des conséquences d'un dysfonctionnement indépendamment de toute mesure de sécurité. Ce risque est identifié lors de l'atelier de catégorisation.
Risque résiduel	Le risque résiduel est le risque subsistant après le traitement du risque ou après que des mesures de protection aient été prises. Ces risques peuvent être identifiés par plusieurs moyens, notamment dans le cadre d'un projet d'acquisition ou de développement et lors de l'analyse d'un incident de sécurité.
Système d'information	Ensemble des actifs informationnels, des ressources humaines et des actifs physiques regroupés sous forme de système pour représenter un fonctionnement permettant d'atteindre un ou des objectifs d'affaires.
Système critique	Système d'information, qui a été identifié critique lors du processus de catégorisation.
Utilisateur	Toute personne physique (enseignant, chercheur, étudiant, diplômé, personnel administratif, retraité, consultant), ou toute entité morale pour qui un code d'identification et un mot de passe ont été émis pour l'accès aux ressources informationnelles du CHUSJ.

Version	1.0
Statut	Version final
Fichier	Politique sur la sécurité de l'information POL-243
Emplacement	P:\Projet\Architecture de securite\3. ASAI\3.1 Gouvernance\3.1.1.7 Pour envoi_CODI\Politique sur la sécurité de l'information POL-243.doc
Date de création	2018-04-11
Date de la version	2018-05-28
Approuvé par	Comité de direction
Date d'approbation	2018-05-29