INSTITUT DE CARDIOLOGIE DE MONTRÉAL

SUJET : Sécurité de l'information	**POLITIQUE N° : DRTI-SAI-01**

1. PRÉAMBULE

L'Institut de Cardiologie de Montréal (ICM) 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 légale, administrative ou économique.

2. DÉFINITIONS

2.1. Actif informationnel

Système d'information, banque d'information, réseau de télécommunications, technologie de l'information, une infrastructure technologique ou un ensemble de ces éléments ainsi qu'une composante informatique d'un équipement médical spécialisé ou ultraspécialisé, tout document imprimé (papier) généré par les technologies de l'information ou tout autre document papier reconnu par l'ICM.

De façon plus particulière à la présente directive, ces actifs informationnels peuvent être, à titre d'exemple et sans s'y limiter : les ordinateurs, les appareils mobiles, les logiciels, les applications, le courrier électronique, l'internet et l'intranet (le cas échéant) ainsi que tout autre outil informatique mis à la disposition des utilisateurs.

2.2. Réseau

Ensemble des organismes du ministère de la Santé et des Services sociaux (MSSS) 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).

2.3. Cadre normatif de la sécurité de l'information du Réseau

Ensemble de textes encadrant la sécurité de l'information, incluant la Politique provinciale de sécurité de l'information (PPSI), le Cadre de gestion de la sécurité de l'information (CGSI) du MSSS, les règles particulières sur la sécurité organisationnelle du MSSS, les guides et procédures qui s'y rattachent.

2.4. Confidentialité

Propriété que possède une donnée ou une information de n'être accessible, ni divulguée qu'aux personnes ou entités désignées et autorisées.

2.5. Disponibilité

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

2.6. 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.

2.7. Authentification

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

2.8. Irrévocabilité

Propriété d'un acte d'être définitif et qui est clairement attribué à la personne qui l'a posé ou au dispositif avec lequel cet acte a été accompli.

2.9. Détenteur de l'information

Un employé désigné par l'ICM, 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.

2.10. Médias sociaux

Toute forme d'application, plateforme et média virtuel en ligne visant l'interaction sociale la collaboration, la création et le partage de contenu.

Les médias sociaux sur Internet comprennent notamment :

- Les sites sociaux de réseautage.
- Les sites de partage de vidéos ou de photographies.

- Les sites de microblogage.
- Les blogues.
- Les forums de discussion.
- Les encyclopédies en ligne.

2.11. Utilisateur

Toute personne de l'ICM 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'ICM ou y a accès.

2.12. Patient

Toute personne qui a reçu, aurait dû recevoir, reçoit ou requiert des services de l'établissement, d'une ressource intermédiaire ou d'une ressource de type familial ou de tout autre organisme, société ou personne auquel l'établissement a recourt pour la prestation de services par entente visée à l'article 108 de la Loi sur les services de santé et les services sociaux (LSSSS). Le terme Patient désigne l'usager au sens de la LSSSS.

3. OBJECTIFS

Orienter et déterminer l'utilisation appropriée et sécuritaire de l'information papier ou électronique, des technologies de l'information et des télécommunications et, plus spécifiquement, d'assurer :

- Le respect de la vie privée des individus, notamment, la confidentialité des renseignements à caractère nominatif relatifs aux patients et au personnel de l'ICM.
- La conformité aux lois et règlements applicables ainsi que les directives, normes et orientations gouvernementales et, plus particulièrement, permettre de respecter les prescriptions du cadre normatif de la sécurité de l'information du Réseau quant aux renseignements nominatifs et aux informations à caractère confidentiel transmis ou conservée à l'aide d'actifs informationnels.
- La disponibilité, l'intégrité, la confidentialité, l'authentification et l'irrévocabilité à l'égard de l'ensemble des activités d'accès, d'utilisation, de collecte, d'enregistrement, de traitement, de conservation, de diffusion et de transmission des actifs informationnels de l'établissement, de même que la continuité des services.

- La sécurité de l'information en regard de l'utilisation des réseaux informatiques, du réseau intégré de télécommunications multimédia (RITM), de l'Internet notamment des médias sociaux.
- Une conduite rigoureuse de tout utilisateur face aux actifs informationnels sensibles pour les fins cliniques, de recherche, d'enseignement, d'études et de statistiques.
- Le respect du code d'utilisation éthique des actifs informationnels et des médias sociaux *(voir Annexe B).*
- Préserver l'image et la crédibilité de l'établissement auprès des patients et de la population.
- Sensibiliser tout utilisateur sur l'exercice de ses libertés et de ses droits fondamentaux dans le respect de ceux d'autrui et du bien-être général.
- Sensibiliser tout utilisateur aux problématiques pouvant se poser en raison de l'utilisation de moyens de réseautage individuel.
- Mettre en œuvre des mesures préventives et dissuasives pour assurer un environnement respectueux des libertés de moyens de réseautage virtuel.

4. CHAMP D'APPLICATION

4.1. Les personnes visées

La présente politique s'applique à toute personne physique ou morale, dont tous les fournisseurs, contractuels, chercheurs, stagiaires et entités externes, dûment autorisée à avoir accès aux actifs informationnels détenus par l'ICM.

4.2. Les actifs et services visés

- les actifs informationnels de l'ICM détenus dans l'exercice de sa mission, que sa conservation soit assurée par l'ICM ou par un tiers.
- les contrats et les ententes de services en lien avec des actifs informationnels.
- toute information traitée électroniquement et/ou conservée sur papier.

5. ÉNONCÉS ET PRINCIPES GÉNÉRAUX

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.

5.1. Responsabilité et imputabilité

- Le plus haut dirigeant d'un organisme 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 organisme.
- Les organismes du Réseau sont responsables devant le ministre de la Santé et des Services sociaux et conservent leurs responsabilités dans toute forme d'impartition. À ce titre, ils précisent leurs exigences en matière de sécurité de l'information dans toute entente ou contrat signé avec un partenaire interne ou externe.
- Toute personne, autorisée à avoir accès aux actifs informationnels de l'ICM 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 plus haut dirigeant de l'ICM.

5.2. Sensibilisation et formation

- Un programme continu de sensibilisation et de formation à la sécurité de l'information doit être mis en place.
- Des activités de sensibilisation et de formation des 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 doivent être effectuées.

5.3. Droit de regard

L'ICM se réserve un droit de regard sur tout usage des actifs informationnels de l'établissement.

6. RÔLES ET RESPONSABILITÉS

- La structure fonctionnelle de la sécurité de l'information de l'ICM est ainsi que les rôles et responsabilités des principaux intervenants en sécurité de l'information sont définis dans le CGSI (*voir Annexe A*) qui vient compléter les dispositions de la présente politique.

- Le responsable de la sécurité de l'information, délégué par le président-directeur général, est responsable de l'application de la politique de sécurité de l'information.

7. SANCTIONS

Lorsqu'un utilisateur ou une organisation 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.

8. DISPOSITIONS FINALES

- La présente politique entre en vigueur à la date de son approbation par le Comité de direction (Comité exécutif).
- Cette politique est réévaluée minimalement aux trois ans afin d'intégrer les nouveaux besoins, les nouvelles pratiques, les nouvelles menaces et les nouveaux risques encourus.

INSTITUT DE CARDIOLOGIE DE MONTRÉAL

ANNEXE A

CADRE DE GESTION

DE LA SÉCURITÉ DE L'INFORMATION

Liste des acronymes

CA	Conseil d'administration
CSI	Comité de sécurité de l'information
CGSI	Cadre de gestion de la sécurité de l'information
DRI	Dirigeant réseau de l'information
ICM	Institut de cardiologie de Montréal
LGGRI	Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement
MSSS	Ministère de la Santé et des Services sociaux
ROSI	Responsable organisationnel de la sécurité de l'information
RSI	Responsable de la sécurité de l'information
SCT	Secrétariat du Conseil du Trésor

1. PRÉAMBULE

L'Institut de cardiologie de Montréal (ICM) 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 légale, administrative ou économique.

Le Cadre de gestion de la sécurité de l'information (CGSI) décrit les rôles et responsabilités en matière de sécurité de l'information, lesquels étaient auparavant intégrés à la politique.

2. DÉFINITIONS

2.1. **Actif informationnel**

Système d'information, banque d'information, réseau de télécommunications, technologie de l'information, une infrastructure technologique ou un ensemble de ces éléments ainsi qu'une composante informatique d'un équipement médical spécialisé ou ultraspécialisé, tout document imprimé (papier) généré par les technologies de l'information ou tout autre document papier reconnu par l'ICM.

De façon plus particulière à la présente directive, ces actifs informationnels peuvent être, à titre d'exemple et sans s'y limiter : les ordinateurs, les appareils mobiles, les logiciels, les applications, le courrier électronique, l'internet et l'intranet (le cas échéant) ainsi que tout autre outil informatique mis à la disposition des utilisateurs.

2.2. **Détenteur de l'information**

Un employé désigné par l'ICM, 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.

2.3. **Réseau**

Ensemble des organismes du ministère de la Santé et des Services sociaux (MSSS) 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).

2.4. **Le Dirigeant réseau de l'information (DRI)**

Conformément au cadre gouvernemental de gestion de la sécurité de l'information du Secrétariat du Conseil du trésor (SCT), le DRI (relevant du ministère) a pour mandat de veiller à l'application, par les organismes publics qui relèvent de lui, des règles de gouvernance et de gestion établies en matière de sécurité de l'information.

2.5. **Le Responsable organisationnel de la sécurité de l'information (ROSI)**

Le ROSI (relevant du MSSS) agit à titre de porte-parole du dirigeant principal de l'information du SCT auprès du Réseau. À ce titre, il communique les orientations et les priorités d'intervention gouvernementales en matière de sécurité de l'information. Il assiste le sous-ministre dans la détermination des orientations stratégiques et des priorités d'intervention en matière de sécurité de l'information et le représente lors d'incidents de sécurité de l'information à portée gouvernementale.

2.6. **Système d'information**

Système constitué des ressources humaines (le personnel), des ressources matérielles (l'équipement) et des procédures permettant d'acquérir, de stocker, de traiter et de diffuser les éléments d'information pertinents pour le fonctionnement d'une entreprise ou d'un organisme.

2.7. **Utilisateur**

Toute personne de l'ICM 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'ICM ou y a accès.

3. OBJECTIFS

Le CGSI complète les dispositions de la politique de la sécurité de l'information de l'ICM par la mise en place d'une structure fonctionnelle de la sécurité de l'information et par la définition des rôles et responsabilités en la matière.

Les rôles et responsabilités définis dans le CGSI concernent l'approbation, la mise en place, la coordination, le développement, le suivi et l'évaluation de la sécurité de l'information à l'ICM, en tenant compte des exigences du cadre légal et administratif applicable au Réseau du MSSS et des principes généraux de la politique provinciale de sécurité de l'information du Réseau du MSSS.

4. RÔLES ET RESPONSABILITÉS

4.1. **Le Conseil d'administration (CA) de l'ICM :**

1. adopte la présente politique et le plan d'action établis par l'ICM en matière de sécurité de l'information, s'assure de sa mise en œuvre et du suivi de son application;
2. reçoit et entérine annuellement ou au besoin le Bilan de sécurité de l'information de l'ICM.

4.2. **Le président-directeur général :**

1. s'assure que les valeurs et orientations en matière de sécurité soient partagées à l'ensemble des gestionnaires, du personnel, des médecins, des étudiants et des chercheurs;
2. s'assure du respect des lois et des règles de sécurité de l'information s'appliquant au Réseau, notamment celles émises par le SCT;
3. s'assure qu'un bilan annuel de sécurité soit présenté au CA ;
4. nomme le responsable de la sécurité de l'information et s'assure de lui octroyer les pouvoirs et ressources nécessaires à la réalisation de ses tâches et responsabilités;
5. s'assure de la nomination des détenteurs de la sécurité de l'information pour l'ICM afin d'assurer la sécurité de l'information et des ressources qui la sous-tendent;
6. s'assure de la mise en place d'un comité chargé de la sécurité de l'information à l'ICM et mandate le Responsable de la sécurité de l'information (RSI) pour présider ce comité;
7. approuve le CGSI de l'ICM;
8. s'assure de la mise en œuvre de la politique de sécurité de l'information adoptée par le CA et des rôles et responsabilités du cadre de gestion de la sécurité de l'ICM;
9. s'assure de la gestion adéquate des risques de sécurité de l'information en lien avec son contexte organisationnel.

4.3. **Le responsable de la sécurité de l'information (RSI) :**

1. veille à l'élaboration, au maintien et à l'application de la politique sur la sécurité de l'information;
2. est responsable de l'élaboration du Plan directeur de sécurité et assure sa mise en œuvre et son suivi;
3. planifie les activités nécessaires à la mise en place de la sécurité de l'information au sein de l'ICM;
4. met en place le Comité de sécurité de l'information (CSI). Le comité est présidé par le RSI ou son délégué;
5. s'assure de l'élaboration et de la mise en œuvre d'un programme formel de formation et de sensibilisation en matière de sécurité de l'information;
6. s'assure de la mise en place du registre d'autorité de la sécurité de l'information, dans lequel sont notamment consignés les noms des détenteurs de l'information et les systèmes d'information qui leur sont assignés;
7. veille à transmettre les besoins des détenteurs en matière de sécurité au CSI;

8. s’assure de la mise en œuvre d’un processus de gestion des incidents de sécurité de l’information à l'ICM;
9. veille à la mise en œuvre de toute recommandation jugée pertinente découlant d’une vérification ou d’un audit de sécurité;
10. s’assure de la production d’un bilan annuel ou, au besoin, d’un plan d’action triennal de la sécurité de l’information pour l'ICM, les valide et les transmet au ROSI du Réseau et à son dirigeant;
11. représente l'ICM au Comité provincial de la sécurité de l’information du Réseau et s’assure de la participation de l'ICM aux processus provinciaux de gestion de la sécurité de l’information ;
12. agit à titre de porte-parole du ROSI auprès de l'ICM en informant les différents intervenants en sécurité de l’information, des orientations et des priorités d’intervention provinciale et s’assure de leur mise en œuvre ;
13. s’assure de l’encadrement de la sécurité de l’information au sein de l'ICM, veille à l’application de la politique et du CGSI de l'ICM et s’assure du respect par l'ICM, des règles particulières publiées par le DRI en matière de sécurité de l’information ;
14. dirige la coordination et la cohérence des activités de sécurité de l’information menées à l'ICM, notamment ceux de son officier de sécurité de l’information et de son conseiller en gouvernance de la sécurité, le cas échéant ;

4.4. **Le conseiller en gouvernance de la sécurité :**

Le conseiller en gouvernance de la sécurité de l’information apporte son soutien au RSI de l'ICM, notamment en ce qui concerne l’encadrement de la sécurité de l’information, le choix des moyens pour rencontrer les exigences des règles particulières adoptées par le DRI et la planification des actions en sécurité. À cet égard, il :

1. accompagne le RSI dans la définition des orientations stratégiques, des directives et des plans d’action en matière de sécurité de l’information;
2. participe à la rédaction des documents d’encadrement de la sécurité de l’information de l'ICM;
3. accompagne le RSI dans la mise en œuvre des orientations internes découlant des directives ministérielles et celles du DRI, des politiques internes et des pratiques généralement admises à cet égard;
4. participe à la définition et accompagne le RSI dans la mise en œuvre de processus formels de gestion de la sécurité de l’information;
5. accompagne les directions partenaires en matière de sécurité de l’information et participe à l’intégration de dispositions garantissant le respect des exigences de sécurité de l’information dans les ententes de service et les contrats;
6. assiste les détenteurs de l’information dans la catégorisation de l’information relevant de leur responsabilité, dans l’identification et l’évaluation des situations de risques ainsi que dans la définition de plans d’action visant à réduire les risques de

sécurité de l'information à un niveau acceptable pour l'ICM et pour le MSSS;

7. identifie et prend en charge les exigences de sécurité de l'information lors de la réalisation de projets de développement ou de l'acquisition de systèmes d'information;
8. élabore et met en œuvre le programme de formation et de sensibilisation en matière de sécurité de l'information;
9. tient à jour le registre d'autorité de la sécurité de l'information;
10. assure la coordination et la réalisation de projets de sécurité de l'information;
11. produit les bilans et les plans d'action de sécurité de l'information de l'ICM.

4.5. **L'officier de sécurité de l'information:**

L'officier de sécurité de l'information est un professionnel de la sécurité de l'information ayant les compétences nécessaires à la réalisation des tâches et responsabilités suivantes. Il :

1. contribue à la mise en place des activités opérationnelles de sécurité de l'information, plus précisément, la planification, le déploiement, l'exécution, la surveillance, les enquêtes et l'amélioration des processus de sécurité nécessaires à la gestion opérationnelle de la sécurité à l'ICM, la gestion des risques et la gestion des incidents en respectant les exigences de sécurité définies dans les règles particulières et conformément aux pratiques recommandées de l'industrie;
2. participe activement au réseau d'alerte du Réseau pour la gestion des incidents de sécurité de l'information;
3. contribue aux analyses de risques de sécurité de l'information, identifie les menaces et les situations de vulnérabilité et met en œuvre les solutions appropriées;
4. soutient le RSI et le conseiller en gouvernance de la sécurité dans les activités de développement et d'acquisition, pour le volet technique de la sécurité dans le respect des exigences de sécurité définies dans les règles particulières et conformément aux pratiques recommandées;
5. participe aux comités de gestion des changements, s'il y a lieu, et possède un droit de réserve face à des changements qu'il juge trop risqués sur le plan de la sécurité de l'information;
6. s'assure de la production des rapports des processus de sécurité de l'information (incidents, vulnérabilités, etc.).

4.6. **Le Comité de sécurité de l'information (CSI) :**

1. constitue un mécanisme de coordination et de concertation qui, par sa vision globale, est en mesure de proposer des orientations en matière de sécurité;
2. est formé minimalement du RSI ou de son délégué, conseiller en gouvernance de la sécurité, de l'officier de sécurité de l'information, du responsable de l'application de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, d'un responsable en technologies de l'information, de gestionnaires et de détenteurs d'actifs informationnels;
3. formule ses recommandations au RSI au regard de l'élaboration, de la mise en œuvre et de la mise à jour des mesures prévues au plan directeur de la sécurité, conformément au Cadre normatif de la sécurité de l'information du Réseau;
4. évalue l'incidence des nouveaux projets sur la sécurité de l'organisation.

4.7. **Le chef du service des archives médicales et le responsable de la gestion des risques** partagent conjointement, avec l'officier de sécurité de l'information, la gestion des incidents et assurent l'application de la procédure de gestion des incidents relatifs à la sécurité et à la confidentialité des actifs informationnels. Chacune des parties intervient strictement dans le cadre des incidents reliés à son domaine de compétence et de responsabilité.

4.8. **Le responsable de l'accès aux documents des organismes publics et de la protection des renseignements personnels** a un rôle-conseil auprès du RSI afin de s'assurer que les mécanismes de sécurité mis en place permettent de respecter les exigences de la Loi sur l'accès aux documents des établissements publics et sur la protection des renseignements personnels.

4.9. **Les gestionnaires :**

1. s'assurent que tout le personnel est informé de leurs obligations découlant de la présente politique;
2. informent leur personnel des normes, directives et procédures de sécurité en vigueur;
3. mettent en place les moyens facilitant la formation et la sensibilisation des utilisateurs quant à l'importance de la sécurité de l'information;
4. s'assurent que les moyens de sécurité soient utilisés de façon à protéger l'information utilisée par leur personnel;
5. communiquent au RSI ou à l'officier de sécurité de l'information tout problème de sécurité qu'ils jugent important et participent à l'application de la procédure de gestion des incidents.

4.10. **Les détenteurs d'actifs informationnels:**

1. sont responsables de leur actif et en suivent l'état de la sécurité. Ils s'assurent que les mesures de sécurité appropriées soient élaborées et suivies;
2. informent le RSI de l'existence de leur actif et de sa sensibilité;
3. s'impliquent dans l'évaluation des risques, la détermination du niveau de protection visé, l'élaboration des contrôles non informatiques, la prise en charge des risques résiduels, la relève et la continuité du processus d'affaires associé à l'actif;
4. déterminent les règles d'accès aux actifs dont ils assument la responsabilité;
5. définissent les limites raisonnables de la disponibilité, de l'intégrité et de la confidentialité pour leurs actifs, en conformité avec le Cadre normatif de la sécurité de l'information du Réseau.

4.11. **Les pilotes de systèmes :**

1. ont la responsabilité de s'assurer du fonctionnement sécuritaire d'un actif informationnel dès sa mise en exploitation, de contrôler et d'autoriser l'accès logique à tout actif informationnel dont ils ont la responsabilité d'utilisation;
2. informent les utilisateurs de leurs obligations face à l'utilisation des systèmes d'information dont ils sont responsables lors de l'attribution des accès.

4.12. **Le personnel utilisateur :**

1. est responsable de respecter la présente politique, normes, directives et procédures en vigueur qui en découlent et d'informer le RSI ou l'officier de sécurité de l'information de toute violation des mesures de sécurité dont ils pourraient être témoins ou de toutes anomalies décelées pouvant nuire à la sécurité des actifs informationnels;
2. signe une déclaration d'allégeance et d'engagement à la confidentialité (annexe C);
3. complète le programme de sensibilisation et de formation (en ligne) sur les actifs informationnels;

4.13. **La direction des ressources humaines, des communications et des affaires juridiques :**

1. est responsable d'informer tout nouvel employé ou bénévole, de ses obligations découlant de la présente politique ainsi que des normes, directives et procédures en vigueur en matière de sécurité de l'information;
2. s'assure que tout nouvel employé ou bénévole signe une déclaration d'allégeance et d'engagement à la confidentialité (Annexe C);
3. détermine les règles et la politique à suivre sur les médias sociaux;
4. nomme une ou des personnes autorisées à aller sur les médias sociaux.

4.14 **La direction des services professionnels et la direction de l'enseignement :**

1. sont responsables d'informer tout nouveau médecin ou stagiaire de ses obligations découlant de la présente politique ainsi que des normes, directives et procédures en vigueur en matière de sécurité de l'information;

2. s'assurent que tout nouveau médecin ou stagiaire signe une déclaration d'allégeance et d'engagement à la confidentialité (Annexe C).

INSTITUT DE CARDIOLOGIE DE MONTRÉAL

ANNEXE B

DIRECTIVE DE SÉCURITÉ

CODE D'UTILISATION ÉTHIQUE

DES ACTIFS INFORMATIONNELS

ET DES MÉDIAS SOCIAUX

Liste des acronymes

CGSI	Cadre de gestion de la sécurité de l'information
ICM	Institut de cardiologie de Montréal
LGGRI	Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement
LSSSS	Loi sur les services de santé et les services sociaux
MSSS	Ministère de la Santé et des Services sociaux
PPSI	Politique provinciale de sécurité de l'information
RSI	Responsable de la sécurité de l'information

Directives de sécurité

Code d'utilisation éthique des actifs informationnels et des médias sociaux

1. PRÉAMBULE

Les ressources, services et interconnections accessibles à l'aide des nouvelles technologies ouvrent la voie à de multiples opportunités, mais aussi à de nombreux risques. Pour pallier à ces risques et, afin de s'assurer que l'organisation profite pleinement de ces opportunités, ce document fait état de la directive officielle de sécurité de l'Institut de cardiologie de Montréal (ICM) relativement à l'utilisation éthique des actifs informationnels mis à la disposition des utilisateurs.

1.1. La directive repose sur les principes directeurs suivants :

1. Le respect de la mission et de la réputation d'excellence de l'ICM.
2. Le respect des normes de sécurité tant physiques que logiques et administratives.
3. Le respect de nos politiques de confidentialité relatives aux informations de nos patients et du personnel.
4. L'utilisation optimale des infrastructures et des systèmes à des fins reliées au travail.
5. Les comportements compatibles à l'éthique en vigueur au sein de l'organisation.
6. Le respect des lois en vigueur, règlements et politiques internes par les utilisateurs.

L'ICM se réserve le droit de mettre en vigueur les systèmes de contrôle nécessaires au respect de ces principes.

2. DÉFINITIONS

2.1. Actif informationnel :

Système d'information, banque d'information, réseau de télécommunications, technologie de l'information, une infrastructure technologique ou un ensemble de ces éléments ainsi qu'une composante informatique d'un équipement médical spécialisé ou ultraspécialisé, tout document imprimé (papier) généré par les technologies de l'information ou tout autre document papier reconnu par l'ICM.

De façon plus particulière à la présente directive, ces actifs informationnels peuvent être, à titre d'exemple et sans s'y limiter : les ordinateurs, les appareils mobiles, les logiciels, les applications, le courrier électronique, l'internet et l'intranet (le cas échéant) ainsi que tout autre outil informatique mis à la disposition des utilisateurs.

2.2. Réseau :

Ensemble des organismes du ministère de la Santé et des Services sociaux (MSSS) qui relèvent du dirigeant réseau de l'information 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).

2.3. Cadre normatif de la sécurité de l'information du Réseau :

Ensemble de textes encadrant la sécurité de l'information, incluant la Politique provinciale de sécurité de l'information (PPSI), le cadre de gestion de la sécurité de l'information (CGSI) du MSSS, les règles particulières sur la sécurité organisationnelle du MSSS, les guides et procédures qui s'y rattachent.

2.4. Médias sociaux :

Toute forme d'application, plateforme et média virtuel en ligne visant l'interaction sociale, la collaboration et le partage de contenus.

Les médias sociaux sur Internet comprennent notamment:

- les sites sociaux de réseautage,
- les sites de partage de vidéos ou de photographies,
- les sites de microblogage,
- les blogues,
- les forums de discussions,
- les encyclopédies.

2.5. Utilisateur :

Toute personne de l'ICM 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'ICM ou y a accès.

2.6. Patient :

Toute personne qui a reçu, aurait dû recevoir, reçoit ou requiert des services de l'établissement, d'une ressource intermédiaire ou d'une ressource de type familial ou de tout autre organisme, société, ou personne auquel l'établissement recourt pour la prestation de services par entente visée à l'article 108 de la Loi sur les services de santé et les services sociaux (LSSSS). Le terme Patient désigne le patient au sens de la LSSSS.

3. DESCRIPTION DE LA DIRECTIVE

1. **Les actifs informationnels** sont en place pour être utilisés à des fins reliées au travail.

2. **Sous réserve des normes prévues par la loi**, nul ne doit s'attendre à ce que le caractère privé ou intime de ses communications faites à l'aide des actifs informationnels soit préservé. L'ICM se réserve le droit d'examiner, sans autre préavis, les communications transigeant sur les actifs informationnels et d'en contrôler l'utilisation.

3. En aucun cas**, l'ICM ne peut être tenu responsable** envers l'utilisateur de tout dommage, perte ou conséquence découlant :

   3.1. D'une interruption volontaire ou d'une panne informatique.
   3.2. D'une utilisation fautive ou négligente des actifs informationnels.

4. **Les actifs informationnels doivent être utilisés**

   4.1. Conformément aux diverses lois provinciales et fédérales qui nous régissent.

   4.2. Conformément à toutes les politiques internes connexes de l'ICM, notamment :

      4.2.1. Politique sur la propriété intellectuelle (DG-03).
      4.2.2. Politique sur la sollicitation et vente (DG-06).
      4.2.3. Politique sur l'implication de l'ICM dans des activités de promotion ou de marketing de cause (DG-09).
      4.2.4. Sécurité des données socio-sanitaires informatisées (DG-10).
      4.2.5. Politique pour prévenir et contrer le harcèlement en milieu de travail (DRH-01).
      4.2.6. Politique pour prévenir et contrer les agressions en milieu de travail (DRH-02).
      4.2.7. Politique de la sécurité de l'information (DRTI-SAI-01).

   4.3. D'une manière productive, en utilisant l'outil le plus approprié selon le besoin.

5. **Les actifs informationnels et les médias sociaux ne doivent pas être utilisés**

   5.1. Pour des fins personnelles durant les horaires de travail.

   5.2. Pour harceler un autre membre du personnel de l'ICM ou toute autre personne.

   5.3. Pour nuire à la prestation de travail d'un autre membre du personnel.

   5.4. Pour visionner, télécharger, copier, partager ou expédier des images ou des fichiers érotiques, de pornographie juvénile ou de sexualité explicite, ou dont le contenu a un caractère diffamatoire, offensant, harcelant, haineux, violent, menaçant, raciste, sexiste, ou qui contrevient à l'une des dispositions de la Charte des droits et libertés de la personne (L.R.Q., c. C-12), ainsi que de toute autre loi au Québec.

5.5. Pour transmettre de l'information à caractère syndical sans autorisation préalable de l'ICM.

5.6. Pour exercer des moyens de pression ou soutenir de tels moyens à des fins de manifestation ou d'incitation à des manifestations.

5.7. Pour télécharger des émissions de radio ou télévision en continu.

5.8. Pour télécharger des films ou de la musique.

5.9. Pour participer, regarder ou jouer à des jeux en ligne.

5.10. Pour l'hébergement de sites Web personnels.

5.11. Pour utiliser les TI pour des activités illégales et/ou malhonnêtes.

5.12. Pour utiliser à son profit les TI mises à sa disposition.

5.13. Pour télécharger tout logiciel ou partager ou copier un logiciel installé sur l'équipement auquel l'utilisateur a accès sans une autorisation préalable.

5.14. Pour créer, expédier ou réexpédier tout message électronique ou fichier qui contient un élément qui contrevient aux paragraphes qui précèdent.

5.15. Pour créer, expédier ou réexpédier tout message électronique ou fichier qui est susceptible d'affecter le fonctionnement de l'équipement mis à sa disposition ou d'un réseau local ou gouvernemental auquel il est relié, ou d'engendrer des coûts additionnels à l'employeur.

5.16. Pour créer ou répondre à des chaînes de lettres.

5.17. Pour transmettre, divulguer ou copier de l'information appartenant à l'ICM, sans autorisation préalable.

5.18. Pour télécharger ou transmettre des informations hautement confidentielles ou stratégiques, du matériel breveté ou protégé par les droits d'auteur, marques de commerce, secrets commerciaux ou de recherche ou autres informations ou documents confidentiels ou privés sans autorisation préalable de l'ICM.

5.19. Pour endommager, altérer ou perturber le fonctionnement de systèmes ou d'ordinateurs de quelque façon que ce soit.

5.20. Pour accéder, sans autorisation, à des systèmes ou à des ordinateurs externes.

5.21. Pour procéder à l'installation d'un logiciel (personnel ou non), de modifier la configuration d'un poste de travail sans l'autorisation préalable du responsable de la sécurité de l'information (RSI) et sous la supervision du service informatique et des télécommunications ou du génie biomédical, le cas échéant.

5.22. Pour divulguer des renseignements personnels concernant les usagers de l'établissement, ni même des renseignements qui permettraient de les identifier soit directement ou indirectement.

6. **Tout renseignement informatisé** concernant un patient ou un employé est un renseignement nominatif et doit recevoir le même traitement que le renseignement écrit au dossier «papier».

7. **Les utilisateurs doivent s'assurer de prendre les précautions nécessaires** afin d'éviter que des renseignements de nature confidentielle puissent être interceptés par des tiers.

8. **L'utilisation des fonctions automatiques de réexpédition de courriel** peut mener à la divulgation de données confidentielles ou nominatives surtout si le service visé est sur Internet. Par conséquent, cette pratique est proscrite.

9. **Chaque personne est responsable d'accéder seulement à l'information nécessaire** à l'exécution normale de son travail.

10. Les codes d'identification et les mots de passe ne doivent pas être partagés. Chaque personne est responsable de s'assurer qu'elle procède bien à la sortie du poste de travail lorsque ses tâches sont terminées ou lorsqu'elle s'absente de son poste de travail; tout mot de passe devrait :

    10.1. Demeurer confidentiel ; conséquemment lors de la réception d'un nouveau mot de passe, l'utilisateur doit immédiatement le modifier, que la technologie l'y force ou non.
    10.2. Comporter un minimum de 8 caractères.
    10.3. Être composé de caractères numériques et alphabétiques, minuscules et majuscules.
    10.4. Être modifié, au moins, tous les 90 jours.
    10.5. Être différent des dix (10) derniers mots de passe utilisés pour le code d'accès associé.
    10.6. Ne pas se retrouver dans le dictionnaire.
    10.7. Ne pas correspondre à un nom de l'entourage de l'utilisateur.
    10.8. Être reconfirmé après une période d'inactivité de 60 minutes de l'ordinateur, via un écran de veille activé avec mot de passe.

11. **L'utilisateur qui est autorisé dans le cadre de sa prestation de travail à aller sur les médias sociaux** :

    11.1. Ne doit, en aucun cas, diffuser sur les médias sociaux un contenu qui concerne un ou des usagers de l'établissement.
    11.2. Doit être le premier à corriger une erreur (publication erronée, diffamation ou autres), pour empêcher toute situation conflictuelle pouvant miner la confiance d'autrui envers l'établissement.
    11.3. Doit impérativement faire ressortir les valeurs et engagements de l'établissement dans le contenu qu'elle diffuse, tout en gardant un ton formel, respectueux et professionnel.

Si un doute survient quant à ces critères, la personne autorisée doit demander l'avis de son supérieur.

11.4. Ne doit pas diffuser sur les médias sociaux un contenu qui pourrait concerner ses collègues, sauf s'il obtient l'autorisation écrite de la personne dont il désire faire mention dans une discussion en ligne ouverte.

11.5. Pourrait être tenu personnellement responsable des documents qu'il diffuse sur les médias sociaux, de son contenu dont les vidéos, les extraits sonores et les images. En outre, tout utilisateur autorisé doit veiller au respect du droit d'auteur.

4. RESPECT DE LA DIRECTIVE

1. La surveillance et la journalisation des accès peuvent constituer des moyens utilisés pour s'assurer du bon usage des actifs informationnels.

2. Un gestionnaire peut demander au responsable de la sécurité de l'information qu'une analyse soit faite de l'utilisation des actifs informationnels par le personnel de son service lorsqu'il existe des raisons de soupçonner que cette utilisation n'est pas conforme à cette directive, aux lignes directrices internes ou à la loi. Cette demande écrite doit mentionner les motifs la justifiant ainsi que la période de temps sujet à l'analyse.

3. La mise en œuvre des mesures de gestion et des vérifications prévues dans cette section doit être faite conformément aux lois, dont particulièrement la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et la LSSSS au Cadre normatif de la sécurité de l'information du Réseau appartenant aux organismes du MSSS (volets « Sécurité » et « Protection des renseignements personnels »), les normes et standards du MSSS, et de l'ICM notamment à l'égard de la protection de la vie privée, des renseignements personnels et d'autres renseignements de nature confidentielle.

4. Toute dérogation à la présente directive, y compris toute infraction aux règles concernant la confidentialité et la sécurité, peut mener à l'application de mesures disciplinaires ou administratives, au remboursement des frais inhérents à la cessation du lien contractuel avec l'ICM ou au congédiement, le cas échéant, le tout en conformité avec les conventions collectives et les politiques administratives.

5. Dans tous les cas, l'ICM se réserve tous ses droits de poursuivre en justice l'utilisateur fautif en remboursement des dépenses occasionnées et en dommages et intérêts.

INSTITUT DE CARDIOLOGIE DE MONTRÉAL

ANNEXE C

ENGAGEMENT AU RESPECT

DE LA CONFIDENTIALITÉ ET

À LA PROTECTION DES ACTIFS INFORMATIONNELS

ENGAGEMENT AU RESPECT DE LA CONFIDENTIALITÉ ET

À LA PROTECTION DES ACTIFS INFORMATIONNELS

Considérant que :

- La mission de l'Institut de cardiologie de Montréal (ICM) consiste notamment, à « dispenser des soins et offrir des services de santé» et que de ce fait, l'Institut de Cardiologie de Montréal (ICM) se voit confier par sa clientèle des informations personnelles et confidentielles, nominatives ou à caractère légal, administratif ou économique;
- Dans le cadre de l'exercice de mes fonctions à l'ICM, je peux avoir accès à des données nominatives de nature très sensible (dossier « patient ») et à des données non nominatives qui ont un caractère confidentiel, provenant des activités de l'ICM, d'autres établissements, ou du réseau de la santé et des services sociaux;

Je, soussigné (e) _____,

Titre ou fonction _____,

Numéro employé(e)_____,
(S'il y a lieu)

Nom de l'entreprise_____, objet du contrat_____,
(S'il y a lieu)

m'engage à :

- **Préserver** le caractère **confidentiel** des informations nominatives, au sens de la Loi sur les services de santé et les services sociaux et de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (ci-après désignée la *Loi sur l'accès*), et non nominatives comportant une valeur légale, administrative ou économique dont je pourrais avoir connaissance dans le cadre des activités qui me sont confiées;.

- **Préserver le caractère confidentielle~~s~~** de toutes les informations médicales et nominatives obtenues dans l'exercice de mes fonctions concernant un patient qu'elles soient verbales, écrites, photographiques, électroniques ou autre et ce, même après son décès (les photocopies du dossier ou d'une partie du dossier de le patient sont strictement interdites).

- Maintenir le dossier d'un patient confidentiel et ne pas donner à quiconque au dossier sans le consentement de le patient.

- Acheminer toute demande d'accès au service des archives lorsqu'une telle demande m'est adressée.

- Respecter mes codes de déontologie et d'éthique professionnelle lorsque j'y suis assujetti.

- Respecter le secret professionnel auquel je suis lié et faire preuve de discrétion lorsque j'aborde le cas particulier d'un patient avec un collègue. Entre autre, je m'engage à m'assurer de ne pas identifier le patient directement ou indirectement dans les espaces communs, particulièrement dans les situations suivantes : discussion du cas d'un patient au poste des infirmières en présence d'autres patients ou visiteurs, au cours d'une tournée d'enseignement dans le corridor, dans les ascenseurs, à la cafétéria et devant des visiteurs ou employés autres que les membres de l'équipe soignante.

- Retirer toutes les données nominatives d'un patient (nom, initiales, numéro de dossier, date de naissance, etc.) sur les documents électroniques utilisés à des fins d'enseignement, de présentations scientifiques, de recherche ou autre.

- Respecter les règlements et politiques de l'ICM, notamment la politique de sécurité de l'information.

- Consulter ou traiter des informations nominatives et non nominatives qui sont de nature confidentielle **uniquement si j'y suis autorisé(e)** et seulement lorsque cela est **nécessaire à l'exercice de mes fonctions.**

- **Ne pas divulguer,** transmettre, ni communiquer ou céder **à des tiers** de l'information nominative et non nominative de nature confidentielle qui m'est confiée, ni la reproduire sans y être préalablement autorisé(e).

- Utiliser les outils et systèmes d'information mis à ma disposition **que pour les fins prévues** et autorisées par l'ICM et en lien avec mes fonctions, conformément aux règles

de sécurité de l'ICM. En outre, **ne jamais divulguer mon ou mes mots de passe, ni prêter ma ou mes clés d'accès aux systèmes**.

- **Signaler** immédiatement au responsable de la sécurité de l'information (RSI), ou à mon supérieur, toute situation portée à ma connaissance ou pour laquelle j'ai raison de croire qu'une personne non autorisée a eu accès ou pourrait avoir accès à des informations confidentielles, nominatives ou non.

- Être **personnellement responsable** des documents que je diffuse sur les médias sociaux et sur internet en général, peu importe leur forme. Les informations que je diffuse ne doivent pas porter préjudice à un patient, un utilisateur ou à l'ICM. Je peux être tenu de réparer tout préjudice causé par cette diffusion. En outre, je dois veiller au respect du droit d'auteur.

En tant qu'employé(e) de l'ICM,

je reconnais que le non-respect de cet engagement peut entraîner des sanctions sévères allant jusqu'au congédiement sans préavis. Cet engagement de confidentialité est continue et perdure au-delà du lien d'emploi à l'ICM.

En tant que consultant ou employé de l'entreprise ci-haut mentionné,

Je m'engage sans limite de temps, à ne pas faire usage d'un tel renseignement ou document à une fin autre que celle s'inscrivant dans le cadre des rapports entretenus entre mon employeur avec l'ICM. J'ai également été informé que le défaut de respecter tout et en partie du présent engagement de confidentialité m'expose ou expose mon employeur à des recours légaux, des réclamations, des poursuites et toutes autres procédures en raison du préjudice causé pour quiconque est concerné par le contrat précité. Je confirme avoir lu les termes du présent engagement et en avoir saisi toute la portée.

Signature *Date*

Signature de la personne recevant la déclaration *Date*

Vous devez obligatoirement signer cette déclaration pour accéder aux systèmes d'information. Celle-ci sera conservée à votre dossier, s'il y a lieu.