Centre intégré universitaire de santé et de services sociaux de l'Est-de-l'Île-de-Montréal
Québec

Direction générale adjointe

POLITIQUE

DEMANDES D'ACCÈS AUX ACTIFS INFORMATIONNELS DES UTILISATEURS, AUX OUTILS DE JOURNALISATION ET JOURNAUX D'ACCÈS, PAR LES GESTIONNAIRES DU CIUSSS-EMTL		
Nº Politique : **POL-057**	Responsable de l'application : Responsable de la sécurité de l'information (RSI)	
Nº Procédure découlant : **s.o.**		
Approuvée par : **Comité de direction**	Date d'approbation : **2018-03-27**	Date de révision : **2022-03-27**
Destinataires : Tous les gestionnaires du CIUSSS-EMTL		

1. CONTEXTE

La présente politique a pour objet d'assurer la continuité des services en cas d'absence ou de départ d'un utilisateur et de protéger les actifs informationnels des abus d'utilisation à des fins personnelles et professionnelles, des risques d'accès non autorisés, de la perte, du vol, de l'altération ou de la divulgation à l'insu du CIUSSS de l'Est-de-l'Île-de-Montréal (EMTL).

Les préoccupations du point de vue de la sécurité de l'information comprennent celles qui suivent :

- assurer la continuité des services en cas d'absence ou de départ d'un utilisateur;
- protéger la confidentialité des informations détenues par un utilisateur d'actifs informationnels (définition à la rubrique 4.1) du CIUSSS-EMTL;
- protéger la vie privée du personnel du CIUSSS-EMTL;
- assurer la gestion sécuritaire des accès requis par le supérieur hiérarchique ou le gestionnaire responsable, qui doit investiguer sur un employé ou un tiers utilisateur dont il a la charge, en cas de motif raisonnable de douter de sa loyauté ou de son respect de l'obligation de discrétion envers le CIUSSS-EMTL, ou de son respect des règles internes.

Cette politique est émise dans un contexte régi par les lois, codes et règlements cités en annexe I, notamment la Charte des droits et libertés de la personne, et répond également aux normes et exigences du ministère de la Santé et des Services sociaux (MSSS) à l'égard de la sécurité de l'information.

Des recours peuvent être intentés contre le CIUSSS-EMTL si, pour quelque motif que ce soit, la sécurité des renseignements personnels des usagers, employés ou partenaires du CIUSSS-EMTL est compromise. Les gestionnaires des directions, ainsi que les responsables des accès aux actifs informationnels (Direction des ressources technologiques et détenteurs des actifs informationnels du CIUSSS-EMTL) doivent donc s'assurer de protéger toute information détenue par un utilisateur, en prenant soin de se conformer à la présente politique.

2. CHAMP D'APPLICATION

La présente politique s'applique à tous les gestionnaires en charge d'utilisateurs des actifs informationnels, c'est-à-dire à toute personne œuvrant au sein du CIUSSS-EMTL, de quelque catégorie d'emploi et de statut d'employé que ce soit, les médecins, les médecins résidents, les dentistes, les pharmaciens, les chercheurs, le personnel de soins et services, administratif ou de soutien, les pairs aidants, les stagiaires, les bénévoles, ainsi que toute personne physique ou morale qui, par engagement contractuel ou autrement, utilise un actif informationnel du CIUSSS-EMTL ou y a accès.

L'information visée est celle que le CIUSSS-EMTL détient dans l'exercice de ses fonctions, que sa conservation soit assurée par lui-même ou par un tiers, et qui est sous la responsabilité d'un utilisateur d'actif informationnel du CIUSSS-EMTL.

3. OBJECTIFS

La présente politique a pour objet d'établir les conditions dans lesquelles les gestionnaires peuvent demander l'accès aux systèmes d'information exploités par les utilisateurs (définition à la rubrique 4.6) dont ils ont la responsabilité.

La politique permet d'identifier :

- les principales règles applicables, incluant les règles de protection de la vie privée des employés;
- les actifs informationnels sous la responsabilité d'un utilisateur qui peuvent être accédés par le supérieur hiérarchique ou le gestionnaire responsable du CIUSSS-EMTL;
- les conditions sous lesquelles de tels accès peuvent être autorisés;
- les contrôles de sécurité permettant de protéger les actifs informationnels du CIUSSS-EMTL;
- les entités autorisées à fournir ces accès lorsque les conditions sont remplies.

4. DÉFINITIONS

4.1. Actif informationnel

Un actif informationnel est 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[1].

Un actif informationnel inclut tout document constitué d'information portée par un support papier ou tout type de support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcriptibles sous l'une de ces formes ou en un autre système de symboles[2].

4.2. Détenteurs de l'information (ou d'applications)

Employés désignés par le dirigeant du CIUSSS-EMTL ou son délégué, appartenant à la classe d'emploi de niveau cadre et dont le rôle est, entre autres, de s'assurer de la sécurité de l'information et des ressources qui la sous-tendent, relevant de la responsabilité de leurs unités administratives.

4.3. Renseignements confidentiels (ou information confidentielle)

Sont confidentiels les renseignements personnels au sens de la loi[3], relatifs aux usagers et au personnel du CIUSSS-EMTL, le tout conformément aux lois et règlements en vigueur.

Sont également considérés comme confidentiels au sens de la loi : tout renseignement dont la divulgation aurait des incidences sur les négociations entre organismes publics[4], un secret industriel[5], un renseignement industriel, financier, commercial, scientifique ou technique[6], l'administration de la justice et la sécurité publique[7], les décisions administratives ou politiques[8] et la vérification[9].

4.4. Renseignement personnel[10]

Tout renseignement qui concerne une personne physique et permet de l'identifier. Un renseignement personnel qui a un caractère public en vertu d'une loi n'est pas considéré comme un renseignement personnel aux fins de la politique de sécurité.

Note[11] : Les renseignements personnels suivants ont un caractère public : le nom, le titre, la fonction, la classification, le traitement, les coordonnées du lieu de travail d'un membre d'un organisme public, de son conseil d'administration ou de son personnel de direction.

---

[1] *Loi concernant le partage de certains renseignements de santé, RLRQ c P-9.0-001, art 3 (1◦).*
[2] *Loi concernant le cadre juridique des technologies de l'information, RLRQ c C-1., art 3.*
[3] *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ c A-2.1, art 53 [Loi sur l'accès]*
[4] *Ibid., art 20.*
[5] *Ibid., art 22 (1).*
[6] *Ibid., art 22 (2) et 23.*
[7] *Ibid., art 28 et ss.*
[8] *Ibid., art 30 et ss.*
[9] *Ibid., art 41 et ss.*
[10] *[Loi sur l'accès]*
[11] *[Loi sur l'accès], art 57 (1)*

4.5. Réseau intégré de télécommunications multimédia (RITM)

L'infrastructure privée de communication du Réseau de la santé (RITM) permet l'échange sécuritaire et confidentiel de données entre les différents établissements et professionnels. Le RITM permet également l'accès et le filtrage contrôlés à l'Internet.

La Direction générale des technologies de l'information du ministère de la Santé et des Services sociaux (DGTI-MSSS) assure la gestion opérationnelle du réseau de télécommunications en plus des divers services s'y reliant, notamment : téléaccès (télétravail), visioconférence et accès pour les fournisseurs externes (service F).

4.6. Utilisateur

Toute personne œuvrant au sein du CIUSSS-EMTL, de quelque catégorie d'emploi et de statut d'employé que ce soit, les médecins, les médecins résidents, les dentistes, les pharmaciens, les chercheurs, le personnel de soins et services, administratif ou de soutien, les pairs aidants, les stagiaires, les bénévoles, ainsi que toute personne physique ou morale qui, par engagement contractuel ou autrement, utilise un actif informationnel du CIUSSS-EMTL ou y a accès.

5. ÉNONCÉ

Les rubriques suivantes fournissent au supérieur hiérarchique ou au gestionnaire en charge de l'utilisateur, des éléments pertinents pour la gestion du dossier, ainsi que les règles et conditions pour la demande d'accès aux actifs informationnels requis par la situation.

5.1. Justification des demandes d'accès par les gestionnaires

Les demandes d'accès aux actifs informationnels utilisés par un employé ou par un tiers utilisateur (partenaire, consultant, fournisseur, etc.) sont justifiables par le besoin d'assurer la continuité des services lors d'une absence ou un départ. Les règles suivantes s'appliquent donc pour le remplacement d'un employé ou d'un tiers utilisateur.

Ces demandes sont également justifiables par le besoin d'investigation par un supérieur hiérarchique ou un gestionnaire responsable, qui a un motif raisonnable de douter de la loyauté de l'employé ou du tiers utilisateur dont il a la charge, ou de douter de son respect de l'obligation de discrétion envers le CIUSSS-EMTL, ou de son respect des règles internes.

5.2. Obligations de l'employé envers l'employeur (le CIUSSS-EMTL) quant à la loyauté, à la discrétion et au respect des règles internes

- Au Québec, la loi oblige un employé à agir avec loyauté envers son employeur. L'article 2088 du Code civil du Québec prévoit que : « Le salarié, outre qu'il est tenu d'exécuter son travail avec prudence et diligence, doit agir avec loyauté et honnêteté et ne pas faire usage de l'information à caractère confidentiel qu'il obtient dans l'exécution ou à l'occasion de son travail ».

  En plus de l'obligation de loyauté, une obligation de discrétion découle de cet article, soit le fait de ne pas faire usage des informations confidentielles obtenues dans le cadre de son travail. Ceci signifie qu'un employé doit, entre

autres, protéger l'information confidentielle qu'il obtient ou à laquelle il a accès, être honnête envers son employeur et offrir une prestation de travail pendant les heures de travail rémunérées (pas de vol de temps).

Le devoir de loyauté se fonde sur l'idée qu'un employeur doit pouvoir avoir confiance en son employé, que ce soit sur les lieux de son travail ou ailleurs. Tout employé doit agir avec loyauté envers son employeur, même si ce devoir n'a pas été mis par écrit.

- L'obligation de loyauté et l'obligation de discrétion survivent à la fin du lien d'emploi.

- Si un employé ne respecte pas son obligation de loyauté et/ou son obligation de discrétion et/ou son obligation de respect des règles internes, des mesures disciplinaires doivent être prises et peuvent aller jusqu'au congédiement.

- À moins que cet usage soit justifié par le travail de l'employé ou autorisé par l'employeur, naviguer sur Internet, accéder à des réseaux sociaux (Facebook, Twitter, etc.) ou envoyer des courriels de nature personnelle durant les heures de travail constituent du vol de temps et peuvent donner lieu à des mesures disciplinaires.

- L'équipement informatique fourni par l'employeur est considéré comme un outil de travail. En conséquence, l'employeur peut déterminer les conditions d'utilisation d'Internet, des différents logiciels et de la messagerie électronique.

- Le droit au respect de la vie privée est applicable au travail, même si l'équipement informatique appartient à l'employeur. Mais s'il a un motif raisonnable pour le faire, l'employeur peut vérifier les fichiers, les courriels, les accès aux systèmes d'information et l'activité Internet (historique des recherches, disque dur, etc.), à l'insu de l'employé.

- Un employeur peut imposer des mesures disciplinaires, allant jusqu'au congédiement, à un employé qui n'utilise pas l'Internet, les logiciels ou la messagerie électronique (liste non exhaustive) conformément à sa politique d'utilisation éthique des technologies de l'information, incluant l'Internet.

- Être loyal envers l'employeur signifie que l'employé ne doit pas partager l'information confidentielle à laquelle il a accès dans le cadre de son travail. Il y a plusieurs types d'informations confidentielles que l'employé doit protéger de manière à respecter son devoir de loyauté, notamment :

    - les secrets commerciaux appartenant à l'employeur (par exemple, une découverte d'un projet de recherche non encore publiée);

    - les informations financières non rendues publiques sur l'employeur;

    - de l'information privée sur les usagers;

- de plus, l'employé ne peut pas vendre des informations appartenant à son employeur, ni les utiliser d'une façon à en tirer profit ou à avoir un impact négatif sur l'employeur.

- Le devoir de loyauté oblige tous les employés à protéger l'information confidentielle recueillie dans le cadre de leur emploi, sans qu'il ne soit nécessaire qu'ils signent un engagement à cet effet.

- Lorsque l'employeur demande à l'employé de signer l'entente de confidentialité, cela signifie qu'il veut être certain que l'employé va garder secrète l'information à laquelle il a accès. Cet engagement crée une responsabilité supplémentaire qui dépasse le devoir général de loyauté envers l'employeur. Les conséquences légales peuvent être plus importantes; l'employé pourrait être congédié et/ou poursuivi par l'employeur pour non-respect de son entente de confidentialité.

- En tout temps, l'employé se doit d'être honnête envers son employeur sur ce qui se passe dans son milieu de travail, puisque ceci fait partie de l'obligation de loyauté envers lui.

- Toutefois, il est important de savoir que le devoir de loyauté n'oblige pas l'employé à dénoncer tout ce qui se passe dans son milieu de travail.

- Par contre, tel que stipulé dans la politique de sécurité de l'information du CIUSSS-EMTL (POL-024), tout utilisateur a l'obligation de signaler immédiatement, selon la procédure de déclaration des incidents de sécurité de l'information, tout acte ou situation dont il a connaissance, susceptible de constituer une violation réelle ou présumée des règles de sécurité. Tout utilisateur a également l'obligation de déclarer toute anomalie pouvant nuire à la protection des actifs informationnels du CIUSSS-EMTL.

5.3. Les obligations des tiers utilisateurs envers le CIUSSS-EMTL, quant à la loyauté, la discrétion et le respect des règles internes

- Les tiers utilisateurs, soit tous les utilisateurs du CIUSSS-EMTL qui ne sont pas à l'emploi de l'établissement, mais qui y œuvrent ou ont accès à ses actifs informationnels (tel que défini à la rubrique 4.6), ont des obligations découlant du contrat ou de l'entente intervenue entre l'utilisateur, ou l'employeur ou le responsable externe de l'utilisateur, et le CIUSSS-EMTL.

- Toutefois, le gestionnaire du CIUSSS-EMTL responsable du tiers utilisateur doit s'assurer que le formulaire[12] d'engagement à la confidentialité et au respect de l'éthique à l'égard des actifs informationnels soit dûment signé par le tiers utilisateur. L'engagement du tiers utilisateur s'étend alors également à toutes les obligations indiquées sur ce formulaire.

- De plus, tel que stipulé dans la politique de sécurité de l'information du CIUSSS-EMTL (POL-024), tout utilisateur a l'obligation de signaler

[12] Annexé à la Politique de sécurité de l'information POL-024.

immédiatement, selon la procédure de déclaration des incidents de sécurité de l'information, tout acte ou situation dont il a connaissance, susceptible de constituer une violation réelle ou présumée des règles de sécurité. Tout utilisateur a également l'obligation de déclarer toute anomalie pouvant nuire à la protection des actifs informationnels du CIUSSS-EMTL.

- Si un tiers utilisateur ne respecte pas son obligation de loyauté et/ou son obligation de discrétion et/ou son obligation de respect des règles internes, des mesures doivent être prises en collaboration avec l'employeur ou le responsable externe du tiers utilisateur, et peuvent aller jusqu'à la fin du contrat ou de l'entente, selon ses termes.

5.4. Les obligations de l'employeur d'assurer le respect de la vie privée de l'employé du CIUSSS-EMTL

- Toute personne a droit au respect de sa vie privée, même au travail. L'employeur doit respecter la vie privée de ses employés, mais il peut surveiller et contrôler leur travail s'il a un motif raisonnable de le faire.

- Par exemple, l'employeur peut surveiller les courriels d'un employé s'il a un motif raisonnable de penser que l'employé utilise le courriel ou l'Internet pour d'autres raisons que le travail pendant ses heures de travail et d'une manière déraisonnable.

- Le supérieur hiérarchique pourra être soutenu par son conseiller en relations de travail au besoin. Le gestionnaire requérant qui n'est pas cadre supérieur doit obligatoirement consulter le conseiller en relation de travail, afin de confirmer la validité du ou des motifs d'investigation.

- Si l'employé qui fait l'objet de la demande d'investigation est un cadre, le supérieur hiérarchique qui veut investiguer doit alors obligatoirement consulter son propre supérieur hiérarchique, et faire approuver sa demande par le cadre supérieur de la Direction des ressources humaines, des communications et des affaires juridiques (DRHCAJ).

5.5. Les obligations du CIUSSS-EMTL afin d'assurer le respect de la vie privée du tiers utilisateur

- Le CIUSSS-EMTL considère que le tiers utilisateur a droit au respect de sa vie privée, durant l'accomplissement des fonctions et tâches découlant du contrat ou de l'entente intervenue entre l'utilisateur, ou l'employeur ou le responsable externe de l'utilisateur, et le CIUSSS-EMTL.

- Toutefois, le gestionnaire du CIUSSS-EMTL responsable du tiers utilisateur a le devoir de surveiller et contrôler le travail. Ce gestionnaire peut donc surveiller les courriels d'un tiers utilisateur, s'il a un motif raisonnable de penser par exemple que ce dernier utilise le courriel ou autres accès pour d'autres raisons que le travail ou l'exécution de ses fonctions, ou qu'il y a possibilité de bris de confidentialité ou de non-respect des règles internes.

- Le gestionnaire responsable du tiers utilisateur pourra être soutenu par un cadre supérieur du CIUSSS-EMTL, responsable du contrat ou de l'entente, afin de confirmer la validité du ou des motifs d'investigation.

5.6. Règles assurant le respect des obligations de confidentialité de l'utilisateur (employé ou tiers utilisateur) envers les actifs informationnels du CIUSSS-EMTL utilisés sous sa responsabilité

Afin de respecter les droits et privilèges d'accès de l'utilisateur, ainsi que la confidentialité des informations qu'il utilise sous sa responsabilité, le CIUSSS-EMTL met en place les règles suivantes :

- L'utilisateur ne doit jamais fournir à quiconque ses coordonnées, clés physiques ou clés logiques d'accès aux actifs informationnels qu'il détient, ni à un autre utilisateur (employé, adjoint(e) ou autre collègue), ni à son remplaçant, ni même à un gestionnaire du CIUSSS-EMTL qui lui en fait la demande, et jamais non plus à toute personne externe au CIUSSS-EMTL.

- Afin d'avoir accès aux actifs informationnels d'un utilisateur, le supérieur hiérarchique ou le gestionnaire du CIUSSS-EMTL en charge de l'utilisateur, doit plutôt faire une demande selon la procédure de demandes d'accès, en indiquant l'urgence.

- S'il ne s'agit pas d'une investigation sur la loyauté, la discrétion ou le respect des règles internes d'un employé, le supérieur hiérarchique de l'employé ou le gestionnaire en charge du tiers utilisateur, doit l'informer des accès obtenus à ses actifs informationnels.

5.7. Dans le cadre de la continuité des services, règles pour les demandes d'accès aux actifs informationnels d'un utilisateur (employé ou tiers utilisateur)

- Afin d'assurer la continuité des services (en cas d'absence ou du départ de l'utilisateur), le gestionnaire responsable de l'utilisateur doit faire, aussitôt que possible, une demande d'accès – pour son remplaçant – aux actifs informationnels requis utilisés sous la responsabilité de l'utilisateur, selon la procédure régulière de demande d'accès, à l'équipe ou à la direction concernée.

  Note : Voir également la politique POL-058 sur la gestion des accès aux systèmes d'information et session utilisateur, en ce qui concerne la révocation des comptes utilisateurs après un départ ou une fin de contrat ou d'entente.

- Dans le cas d'un utilisateur qui n'aura pas de compte d'accès (Windows) au réseau informatique du CIUSSS-EMTL, et ne signera donc pas ce formulaire électroniquement, le supérieur immédiat ou le gestionnaire responsable de l'utilisateur doit s'assurer de faire signer le formulaire d'engagement à la confidentialité et au respect de l'éthique à l'égard des actifs informationnels, avec témoin.

- Lorsque le formulaire d'engagement est signé sur support papier, le numériser et dans le cas d'un employé, le faire suivre à la DRHCAJ pour que ce document soit porté au dossier de l'employé. Dans le cas d'un tiers utilisateur, conserver le formulaire au dossier de la direction responsable.

5.8. Règles pour les demandes d'accès aux actifs informationnels d'un utilisateur dans le cadre d'une investigation (employé ou tiers utilisateur), aux outils de journalisation et journaux sur les accès de l'utilisateur

- Afin de permettre une investigation sur la loyauté, la discrétion ou le respect des règles internes de l'employé, c'est le cadre supérieur, qui s'est assuré du motif raisonnable d'investigation, ou sinon le supérieur hiérarchique accompagné de son conseiller en relations de travail, qui doit-doivent faire la demande d'accès selon la procédure de requête régulière, à l'équipe ou la direction concernée.

- Le supérieur hiérarchique de l'employé ou le gestionnaire en charge de l'utilisateur pourra obtenir un rapport d'accès de l'utilisateur à certaines applications (ou un accès aux journaux si cela est possible dans le cas des applications seulement), un rapport d'accès à l'Internet si disponible, ainsi qu'un accès aux actifs informationnels visés, utilisés sous la responsabilité de l'utilisateur.

- Ces accès auront des privilèges de lecture seulement, sauf exception spéciale autorisée par le responsable de la sécurité de l'information (RSI).

- Les courriels et toute autre information dont l'accès et la consultation ont été autorisés doivent être traités de façon confidentielle (par exemple, conservés dans des fichiers confidentiels). Seul le gestionnaire en cause, ses supérieurs hiérarchiques et le conseiller en relations du travail doivent avoir accès à ces informations.

5.9. Types d'accès qui peuvent être accordés lors d'une demande d'investigation sur la loyauté, la discrétion ou le respect des règles internes de l'utilisateur (liste non exhaustive)

Accès autorisés confidentiellement par l'équipe de sécurité de l'information*:

- accès au compte du logiciel de messagerie et aux courriels
- accès aux répertoires
- accès aux ordinateurs et aux répertoires du disque local « C : »
- accès aux répertoires partagés à l'intérieur du « B : »
- accès aux autres outils informatiques
- visualisation des journaux d'accès de l'utilisateur à l'Internet

- visualisation des listes d'appels et/ou les textos sur cellulaire du CIUSSS-EMTL.

Faire la demande à l'équipe de sécurité de l'information par Octopus.

Accès autorisés confidentiellement par les gestionnaires propriétaires des applications (détenteurs)*:

- accès aux applications et données
- visualisation des journaux d'accès aux applications (dans l'application si permis, ou via un rapport du détenteur de l'application).

Faire la demande via l'équipe de sécurité de l'information par Octopus.

Accès autorisés confidentiellement par la Direction logistique (stationnement)*:

- accès au registre de stationnement (entrées/sorties)
- accès, dans certains cas, à la vidéo de surveillance.

Faire la demande par courriel au Chef de service Logistique-transport.

Accès autorisés confidentiellement par la Direction des services techniques (DST)*:

- accès aux journaux des portes d'accès
- accès, dans certains cas, à la vidéo de surveillance.

Faire la demande au chef de service approprié selon l'installation, ou en contactant le Centre des appels (CDA) par téléphone pour le joindre :

- Noémie Bismuth-Dubois (514-250-9202) HMR et HSCO
  Chef de service sécurité et prévention incendie
- Philippe-André Bergeron (514-251-4000, poste 3330) IUSMM, CLSC, CHSLD et RESM
  Chef de service sécurité et prévention incendie

6. RÔLES ET RESPONSABILITÉS

6.1. La direction générale adjointe – Finances, soutien, administration et performance (DGA-FSAP)

Le comité de sécurité de l'information recommande le contenu de la présente politique au comité de direction via la DGA-FSAP.

6.2. Le comité de direction

Il adopte les politiques de sécurité de l'information établies par le CIUSSS-EMTL et ses mises à jour, et en suit l'application.

6.3. Le responsable de la sécurité de l'information (RSI) du CIUSSS-EMTL

Il veille à la communication, à la compréhension et l'application par les principaux intervenants, les autres responsables désignés et les utilisateurs, des politiques de sécurité de l'information du CIUSSS-EMTL.

6.4. Toutes les directions

Elles sont responsables, notamment, d'informer tout nouveau gestionnaire oeuvrant au sein du CIUSSS-EMTL ou tout nouveau fournisseur ou partenaire du CIUSSS-EMTL, sous leur responsabilité, dès son accueil ou le début de son mandat, de ses obligations découlant des politiques en vigueur en matière de sécurité de l'information.

6.5. La direction des ressources technologiques (DRT)

La DRT est responsable d'émettre les procédures complémentaires à la présente politique, pour le volet technologique, et de veiller à la gestion et à la prise en charge des activités qui la concerne, découlant de cette politique.

6.6. Les directions des services techniques et de la logistique

La DST et la direction Logistique sont responsables d'émettre les procédures complémentaires à la présente politique et de veiller à la gestion et à la prise en charge des activités qui la concerne, découlant de cette politique.

6.7. Les détenteurs d'actifs informationnels

Ils sont responsables de la gestion des accès et des contrôles de sécurité à mettre en œuvre pour les actifs informationnels sous leur responsabilité.

6.8. Les utilisateurs

Tel que stipulé à la politique de sécurité de l'information du CIUSSS-EMTL (POL-024), les utilisateurs ont l'obligation de se conformer aux politiques, procédures et règlements du CIUSSS-EMTL.

Ils ont également l'obligation de signaler immédiatement selon la procédure de déclaration d'incident de sécurité de l'information, tout acte ou situation dont ils ont

connaissance et susceptible de constituer une violation réelle ou présumée des règles de sécurité, ainsi que toute anomalie pouvant nuire à la protection des actifs informationnels du CIUSSS-EMTL.

Note : Les responsabilités, obligations et droits des utilisateurs leur seront communiqués directement par des documents et diffusions à leur intention, séparément de la présente politique s'adressant aux gestionnaires.

7. ÉLABORATION, RÉDACTION ET MISE À JOUR DE LA POLITIQUE

7.1. Le responsable de la sécurité de l'information (RSI)

Le RSI est responsable de s'assurer de l'élaboration, de la rédaction et de la mise à jour de la politique.

7.2. Le comité de sécurité de l'information

Les membres du comité de sécurité de l'information ont participé à la validation de la politique, et participent à la validation de sa mise à jour.

7.3. Calendrier de révision de la politique

La présente politique devra être révisée tous les 4 ans ou plus rapidement en fonction des besoins.

8. RESPONSABLE DE LA MISE EN APPLICATION

8.1. Le responsable de la sécurité de l'information (RSI) du CIUSSS-EMTL

Il est responsable de la mise en application de la présente politique.

9. ENTRÉE EN VIGUEUR

La présente politique entre en vigueur le jour de son adoption par le comité de direction et annule, par le fait même, toute autre politique en cette matière adoptée antérieurement dans l'une ou l'autre des installations administrées par le CIUSSS-EMTL.

10. ANNEXE(S)

ANNEXE 1 – Cadre légal et administratif de la sécurité de l'information.

ANNEXE I - Cadre légal et administratif de la sécurité de l'information

La présente politique s'inscrit principalement dans un contexte régi par les lois, codes et règlements suivants :

Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, RLRQ c G-1.03

Loi concernant le cadre juridique des technologies de l'information, RLRQ c C-1.1

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ c A-2.1

Loi sur les services de santé et les services sociaux, RLRQ c S-4.2

Loi modifiant l'organisation et la gouvernance du réseau de la santé et des services sociaux notamment par l'abolition des agences régionales, RLRQ c O-7.2

Code des professions, RLRQ c C-26

Règlement sur la diffusion de l'information et sur la protection des renseignements personnels, RLRQ c A-2.1, r 2

Charte des droits et libertés de la personne, RLRQ c C-12

Code civil du Québec, RLRQ c CCQ-1991

Loi sur les archives, RLRQ c A-21.1

Code criminel, LRC 1985, c C-46.