OBJET :	POLITIQUE DE SÉCURITÉ DE L'INFORMATION DU CHU DE QUÉBEC-UNIVERSITÉ LAVAL	**POLITIQUE N^{O} 271-30**
DESTINATAIRES :	Tous les utilisateurs des actifs informationnels du CHU de Québec-Université Laval	
ÉMISE PAR :	La Direction générale	
APPROUVÉE PAR :	Le conseil d'administration	
Références :	*Politique provinciale de sécurité de l'information,* Direction générale des technologies de l'information, ministère de la Santé et des Services sociaux (n^{o} MSSS-POL01) *Cadre de gestion sur la sécurité de l'information*, Direction générale des technologies de l'information, ministère de la Santé et des Services sociaux (n^{o} MSSS-CDG01) *Règle particulière sur la sécurité informationnelle*, Direction générale des technologies de l'information, ministère de la Santé et des Services sociaux.	

1. OBJET

La présente politique de sécurité de l'information vise à établir les règles relatives à la mise en place d'un ensemble de mesures de sécurité et de contrôle afin de protéger tous les renseignements personnels et confidentiels, tant sur support papier que sur support électronique. Elle est le premier jalon d'un cadre de gestion de la sécurité de l'information. De plus, elle établit les mesures de sécurité logiques, physiques, humaines et organisationnelles à appliquer et elle détermine les comportements à adopter afin de s'assurer de l'utilisation appropriée des actifs informationnels et des différentes informations pour l'ensemble des utilisateurs.

2. CADRE JURIDIQUE ET ADMINISTRATIF

Les principes directeurs qui sous-tendent la présente politique sont tirés de la Politique provinciale de sécurité de l'information ratifiée en 2015, du Cadre de gestion sur la sécurité de l'information ainsi que de la Règle particulière sur la sécurité organisationnelle du MSSS.

La règle particulière du MSSS précise les orientations et les obligations que doivent respecter les établissements du réseau de la santé et des services sociaux en matière de sécurité de l'information. Cette règle est basée sur la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ, c. M-19.2, a. 5.2), la *Loi sur le Ministère de la Santé et des Services sociaux* (RLRQ, c. M-19.2, a. 5.2) et sur la *Loi concernant le partage de certains renseignements de santé* (RLRQ, c. P-90001, a. 4 et 5). De plus, la *Loi sur la santé et les services sociaux* (RLRQ, c. S-4.2) détermine le rôle d'un établissement de santé, traite également de la sécurité des actifs informationnels (AI) puisque l'utilisation des technologies de l'information est essentielle pour la réalisation des missions des établissements de santé et de services sociaux.

Cette politique est le résultat de la collaboration du CHU de Québec-Université Laval (CHU), du Centre intégré universitaire de santé et de services sociaux de la Capitale-Nationale (CIUSSS-CN), de l'Institut universitaire de cardiologie et de pneumologie de Québec-Université Laval (IUCPQ) et du Centre intégré de santé et de services sociaux de Chaudière-Appalaches (CISSS-CA). Cette collaboration a notamment pour but d'établir une approche concertée en matière de gestion de la sécurité de l'information et de partage régulier d'informations entre des intervenants issus de mêmes professions.

3. CHAMP D'APPLICATION

La présente politique s'applique à toute personne physique ou morale dûment autorisée à accéder aux actifs informationnels détenus par l'établissement, peu importe la localisation de l'actif.

Elle concerne l'information que l'établissement détient dans l'exercice de sa mission, et ce, que sa conservation soit assurée par lui-même ou par un tiers.

4. DÉFINITIONS

4.1. ACTIF INFORMATIONNEL

Banque d'information, système d'information, réseau de télécommunication, infrastructure technologique ou l'ensemble de ces éléments et composante informatique d'un équipement médical spécialisé ou ultraspécialisé. Tout support papier contenant de l'information est également considéré comme un actif informationnel.

4.2. AUTHENTIFIANT

Information confidentielle détenue par une personne et permettant son authentification.

4.3. AUTHENTIFICATION

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

4.4. CHIFFREMENT

Opération par laquelle est substituée à un texte en clair, un texte inintelligible, inexploitable pour quiconque ne possède pas la clé permettant de le ramener à sa forme initiale.

4.5. CONFIDENTIALITÉ

Propriété d'une information accessible uniquement aux personnes autorisées.

4.6. DÉTENTEUR

Employé désigné par son organisme public, appartenant à la classe d'emploi de niveau cadre ou à une classe d'emploi de niveau supérieur, 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.

4.7. DISPONIBILITÉ

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

4.8. DROIT D'AUTEUR

Droit exclusif de produire ou de reproduire une œuvre ou une partie importante de celle-ci sous une forme matérielle quelconque, de la représenter en public, de la publier, de permettre l'un des actes ci-dessus énumérés ainsi que tous les droits accessoires y afférents, le tout tel que prévu par la *Loi sur le droit d'auteur* (L.R.C. (1985) c. C-42).

4.9. HOLISTIQUE

Toute démarche globalisante où divers éléments, habituellement isolés, sont regroupés et coordonnés pour l'obtention plus efficace d'un résultat visé.

4.10. INCIDENT DE SÉCURITÉ DE L'INFORMATION

Un incident en matière de sécurité de l'information peut être vu comme un évènement qui se produit lorsqu'un risque se concrétise (déni de service, virus, atteinte à la protection des renseignements personnels, usurpation d'identité, etc.)

4.11. INFONUAGIQUE

Modèle informatique qui, par l'entremise de serveurs distants interconnectés par Internet, permet un accès réseau, à la demande, à un bassin partagé de ressources informatiques configurables, externalisées et non localisables, qui sont proposées sous forme de services évolutifs, adaptables dynamiquement et facturés à l'utilisation.

4.12. INTÉGRITÉ

Propriété d'une information ou d'une technologie de l'information de n'être ni modifiée, ni altérée, ni détruite sans autorisation.

4.13. IRRÉVOCABILITÉ

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

4.14. PÉRIPHÉRIQUE

Dispositif matériel distinct de l'unité centrale de traitement d'un ordinateur, auquel il est relié, et pouvant assurer l'entrée ou la sortie de données.

4.15. PRINCIPE DE MOINDRE PRIVILÈGE

Autorisation d'accès restreinte de manière à ce que l'utilisateur ne puisse accomplir que les tâches autorisées et nécessaires à l'exercice de ses fonctions.

4.16. RENSEIGNEMENTS PERSONNELS

Renseignements concernant une personne physique et permettant de l'identifier. Le nom d'une personne physique n'est pas un renseignement personnel, sauf lorsqu'il est mentionné avec un autre renseignement la concernant ou lorsque sa seule mention révélerait un renseignement personnel concernant cette dernière.

4.17. RÉSEAU INTÉGRÉ DE TÉLÉCOMMUNICATION MULTIMÉDIA (RITM)

Principal véhicule d'échange d'information entre les organismes du réseau de la santé et des services sociaux.

4.18. TIERS

Toute personne morale ou physique qui exerce pour l'établissement certaines fonctions hors mission.

4.19. USAGER

Toute personne qui a reçu, aurait dû recevoir, reçoit ou requiert des services de l'établissement; ce terme comprend, le cas échéant, tout représentant de l'usager au sens de l'article 12 de la Loi ainsi que tout héritier ou représentant légal d'un usager décédé.

4.20. UTILISATEUR

Toute personne physique ou morale, groupe ou entité administrative qui fait usage d'un ou de plusieurs actifs informationnels sous la responsabilité de l'établissement, notamment les stagiaires, les résidents, les externes, les chercheurs, les médecins, le personnel, les bénévoles et les tiers.

4.21. VIRUS

Programme malveillant dont l'exécution est déclenchée lorsque le vecteur auquel il a été attaché clandestinement est activé, qui se recopie au sein d'autres programmes ou sur des zones systèmes lui servant à leur tour de moyen de propagation et qui produit les actions malveillantes pour lesquelles il a été conçu.

5. PRINCIPES DIRECTEURS

Le CHU de Québec-Université Laval :

- Reconnait que tout utilisateur ayant accès aux informations assume des responsabilités en matière de sécurité au sein de l'établissement et qu'Il doit respecter et appliquer les principes énoncés dans la politique en étant redevable de ses actions auprès du président-directeur général de son établissement;
- Reconnait que toute information générée par les utilisateurs est la propriété exclusive du CHU de Québec-Université Laval. Le principe du privilège d'accès minimal est appliqué en tout temps lors de l'attribution de l'accès aux actifs informationnels;
- Reconnait que la mise en œuvre et la gestion de la sécurité reposent sur une approche holistique (globale) qui tient compte des aspects humains, organisationnels, financiers, juridiques et techniques et que les mesures de protection, de prévention, de détection et de correction doivent garantir le DICAI des actifs informationnels, de même que la continuité des activités;
- S'assure notamment de prévenir les incidents, les erreurs, la malveillance ou la destruction de renseignements sans autorisation;
- Reconnaît qu'une évaluation périodique des risques et des mesures de protection des actifs informationnels doit être effectuée afin d'obtenir l'assurance qu'il y a une adéquation entre les risques, les menaces et les mesures de protection déployées;

- Ne tolère aucune forme de harcèlement, de violence, d'abus, que ce soit sexuel ou autre, effectuée par le biais des services informatiques mis à la disposition des utilisateurs;
- Reconnait qu'il a sous sa responsabilité des données de nature confidentielle, notamment des renseignements personnels. Par conséquent, il doit prendre les mesures de sécurité propres à assurer la protection des renseignements collectés, utilisés, communiqués, conservés ou détruits.

6. OBJECTIFS DE LA POLITIQUE

Cette politique sert de principale fondation et permet à l'organisme d'assurer le respect de tous les actifs informationnels détenus ou sous sa responsabilité, et ce, selon cinq grands axes de protection, soit la disponibilité, l'intégrité, la confidentialité, l'authentification et l'irrévocabilité (DICAI).

Enfin, elle permet d'assurer :

- Le respect de la vie privée des individus, notamment la confidentialité des renseignements à caractère personnel relatifs aux usagers et aux personnes qui exercent leur fonction ou leur profession au sein de l'établissement;
- La sécurité de l'information en regard de l'utilisation du réseau informatique de l'établissement, notamment le site Internet, l'infonuagique, le courrier électronique du réseau intégré de télécommunication multimédia (RITM);
- La conformité aux lois et aux règlements applicables ainsi qu'aux directives, aux normes et aux orientations gouvernementales;
- La mise en place d'une culture de sécurité de l'information particulièrement par la sensibilisation et la responsabilisation accrue des utilisateurs quant aux risques et aux enjeux entourant l'utilisation de l'information.

7. ÉNONCÉ DE POLITIQUE

7.1. PROTECTION DES RENSEIGNEMENTS PERSONNELS ET CONFIDENTIELS

7.1.1. Respect et droit

- Les utilisateurs doivent respecter l'encadrement légal et réglementaire en matière de protection des renseignements personnels et confidentiels;
- Un utilisateur conserve le droit au respect de sa vie privée et de sa dignité lorsqu'il œuvre au sein de l'établissement. Toutefois, la protection de la vie privée ne limite pas les actions que l'établissement a le droit de prendre afin de gérer, de se protéger, de protéger ses usagers et d'obtenir des renseignements sur ses utilisateurs, et ce, à plus forte raison lorsqu'ils en sont avisés au préalable.

7.1.2. Audits de sécurité

- L'établissement emploie des outils de surveillance, de contrôle et d'enregistrement de toute utilisation de ses actifs informationnels et peut en tout temps analyser et évaluer l'usage qui en est fait;

- Afin de permettre la détection de logiciels malveillants sans angle mort, l'établissement est autorisé à surveiller tout trafic transitant par ses réseaux informatiques, incluant toutes les connexions cryptées. Ceci inclut la surveillance des services courriel en ligne ainsi que tout autre service à usage personnel. Seuls certains sites jugés de confiance absolue sont exempts de ce type d'audit.

7.1.3. Collecte

Il est interdit à tout utilisateur de recueillir un renseignement personnel ou confidentiel si celui-ci n'est pas nécessaire à l'exercice de ses fonctions ou à la mise en œuvre d'un programme dont il a la gestion.

Les utilisateurs doivent s'assurer de respecter la loi, notamment en matière de consentement des usagers.

7.1.4. Accès et utilisation

Les renseignements personnels ou confidentiels doivent être utilisés et ne servir qu'aux fins pour lesquelles ils ont été recueillis ou obtenus. Les privilèges d'accès sont attribués par les personnes autorisées, et le responsable de la sécurité de l'information (RSI) ou les personnes qu'il délègue doit tenir un registre à cet effet. Toute personne utilisant les actifs informationnels mis à sa disposition doit s'assurer que les documents confidentiels, quels que soient leurs supports, soient hors d'atteinte en les conservant en lieu sûr.

Le détenteur de l'information, avec l'appui du responsable de la sécurité de l'information (RSI) ou de toute autre personne autorisée, peut réviser, suspendre ou révoquer un privilège d'accès à un utilisateur notamment pour les raisons suivantes :

- Ne respecte pas la présente politique ou les directives et les procédures qui en découlent;
- S'absente ou n'a pas utilisé ses comptes d'accès depuis plus de 90 jours après une vérification préalable;
- Change de fonction à l'intérieur de l'établissement;
- Termine son contrat ou son assignation;
- Quitte définitivement l'établissement ou est congédié;
- Divulgue des renseignements personnels ou confidentiels pour des raisons autres que celles prévues dans l'exercice de ses fonctions;
- Fait l'objet d'une suspension.

7.1.5. Communication

Tout utilisateur détenant un privilège d'accès s'engage à ne pas divulguer, sauf dans le cadre de ses fonctions, les renseignements personnels ou confidentiels dont il a pu prendre connaissance. Notamment, il est interdit de consulter, de diffuser, de divulguer ou d'imprimer des renseignements concernant les usagers, que ce soit son propre dossier, celui d'un de ses proches ou celui de toute autre personne. En cas de violation de cet engagement, l'établissement peut imposer des sanctions disciplinaires ou administratives (*cf.* section 8.1).

Selon les balises prévues à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1), certains renseignements peuvent ou doivent parfois être protégés et ne pas être accessibles aux citoyens. Il s'agit de renseignements qui pourraient avoir une incidence économique, politique ou légale pour l'établissement. Le responsable de l'accès à l'information évalue ces demandes particulières et applique, si requis, les restrictions à l'accès prévues à la loi.

En vertu de l'article 83 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1) et de l'article 17 de la *Loi sur les services de santé et les services sociaux* (RLRQ, c. S-4.2, art. 17), l'usager a le droit de consulter son dossier ou d'en obtenir une copie. Les systèmes informatiques doivent prévoir cette possibilité; les droits d'accès des usagers demeurent les mêmes que lorsque le dossier est détenu sur support papier (demande faite au Service des archives médicales). Ces accès doivent être possibles quelle que soit la forme des documents (écrite, graphique, sonore, visuelle, informatisée ou autre).

7.1.6. Conservation et destruction

Tout document appartenant à l'établissement doit être conservé et détruit de manière sécuritaire. Tout utilisateur doit respecter les règles en vigueur de même que les procédures qui les accompagnent, puis la structure de classification et le calendrier de conservation de l'établissement.

7.2. UTILISATION D'INTERNET, DU RÉSEAU INTÉGRÉ DE TÉLÉCOMMUNICATION MULTIMÉDIA (RITM) ET DES RÉSEAUX INFORMATIQUES

Les actifs informationnels mis à la disposition des utilisateurs par l'établissement le sont uniquement pour une utilisation professionnelle, plus spécifiquement pour des tâches reliées à l'exercice des fonctions de ses utilisateurs. La présente politique émet des règles dans le but que chacun les traite avec vigilance en respectant les droits d'auteur, la propriété intellectuelle, les règles de licences de logiciels, les droits de propriété, la confidentialité des informations, le bon emploi des ressources et les lois et règlements en vigueur au Québec et au Canada.

Les actifs informationnels et de télécommunication, les outils Internet, le réseau intégré de télécommunication multimédia (RITM) incluant ses réseaux sans fil accessibles à l'aide des réseaux informatiques de l'établissement ne doivent pas être utilisés en violation des lois et des réglementations en vigueur. De plus, l'organisme s'engage à coopérer face à toute requête en provenance des forces de l'ordre ou de tout autre organisme mandaté à cet effet.

<u>L'utilisateur ne doit pas :</u>

- Afficher de document ou de graphique sexuellement explicite, haineux et raciste. De tels documents ne doivent pas être archivés, enregistrés, distribués ou édités à l'aide du réseau de l'établissement;
- Profiter des facilités d'accès à Internet pour propager un virus sur les réseaux informatiques de l'établissement;
- Se servir des facilités d'accès à Internet ou au réseau intégré de télécommunication multimédia (RITM) ou à tout autre moyen pour rendre inutilisable ou surcharger les ordinateurs et le réseau, ou pour contourner les systèmes mis en place pour protéger la vie privée ou la sécurité des actifs informationnels ou des autres utilisateurs;

- Utiliser un modem sur un poste de travail sans l'approbation du RSI;
- Installer ou modifier un actif informationnel sans l'autorisation préalable de la personne désignée par le RSI. Par exemple, l'installation et, par conséquent, l'utilisation de jeux sur les systèmes d'information ne sont pas autorisées;
- Utiliser des périphériques externes pour conserver des documents. Exceptionnellement, avec l'autorisation du RSI ou des personnes qu'il délègue, les utilisateurs peuvent conserver des documents sur des supports amovibles chiffrés (clé USB, disque dur externe);
- N'emmagasiner en aucun cas des informations concernant un usager (photos, résultats de laboratoire, etc.) sur leurs actifs informationnels personnels (portable, téléphone intelligent, infonuagique, clé USB, etc.);
- Divulguer la structure des réseaux d'information de l'établissement, en tout ou en partie;
- Déposer sur Internet (site, dépôt en ligne) des informations personnelles et confidentielles concernant un usager.

L'utilisateur doit :

- Utiliser les codes d'accès ou les mots de passe qui lui ont été assignés à la suite de l'approbation de son supérieur ou de ses délégués. De plus, il est responsable des activités résultant de l'usage de ses codes d'accès et de ses mots de passe. Les mots de passe des utilisateurs sont confidentiels;
- Utiliser uniquement les équipements informatiques portables qui sont la propriété de l'établissement (ex. : tablette électronique, téléphone portable, ordinateur portable) pour communiquer avec le réseau intégré de télécommunication multimédia (RITM);
- Utiliser les appareils personnels (ex. : tablette électronique, ordinateur portable, téléphone intelligent, etc.) sur les réseaux de l'établissement lorsque le RSI leur en a donné l'autorisation à la suite d'une demande d'accès. L'établissement se réserve le droit de configurer ces équipements personnels afin de garantir la sécurité de son réseau informatique et celui du réseau intégré de télécommunication multimédia (RITM);
- Respecter la confidentialité de la connaissance partielle ou totale de la structure des réseaux d'information de l'établissement. De plus, les utilisateurs doivent s'assurer que leur utilisation des réseaux d'information n'altère pas la structure de ceux-ci.

Enfin, l'utilisateur s'engage à rembourser les frais de réparation ou autres frais encourus par l'établissement qui seraient reliés à une utilisation non autorisée, inadéquate ou malveillante dudit actif informationnel, et ce, selon le tarif horaire applicable.

7.3. UTILISATION DU COURRIER ÉLECTRONIQUE

- Les règles d'utilisation du courrier électronique émises dans la *Politique d'utilisation du courrier électronique au CHU de Québec* nº 233-00, font partie intégrante de la présente politique;
- Les utilisateurs ayant des privilèges d'accès au courrier électronique organisationnel doivent l'utiliser uniquement pour des raisons professionnelles;
- La transmission de renseignements personnels ou confidentiels par courrier électronique (Internet, texto ou autre) est interdite, à moins que l'utilisateur n'ait pris les mesures requises de chiffrement prévues par l'établissement. Par ailleurs, l'utilisateur doit également être conscient que les courriers

électroniques qu'il envoie peuvent, à son insu, être redirigés, imprimés, sauvegardés ou affichés sur d'autres médias ou d'autres systèmes informatiques. Les utilisateurs doivent se servir du courrier électronique reconnu par l'organisme permettant le chiffrement;

- Aucune information concernant un usager ne peut être acheminée par courrier électronique (Internet, texto ou autre), à moins :
  - Que ce moyen ait été jugé sécuritaire après qu'une évaluation des risques de sécurité ait préalablement été effectuée par le service de sécurité informationnelle des technologies de l'information;
    - Le formulaire de consentement ainsi que le formulaire de demande de projet pour l'évaluation des risques sont disponibles sur l'intranet de l'établissement.
  - Que l'usager n'ait préalablement consenti par écrit à ce que l'on communique ses informations à d'autres intervenants de la santé ou avec lui par ce moyen, sauf dans les cas où cette communication est autorisée par la loi;
  - Que l'utilisateur respecte les règles de tenue de dossiers de l'établissement;
- La modification d'un message avant sa retransmission à un autre destinataire est interdite;
- L'usage du courrier électronique pour faire des envois massifs de messages sans autorisation est interdit, de même que dans le but de faire de la propagande (syndicale, politique, etc.).

7.4. UTILISATION DES OUTILS PERSONNELS AU TRAVAIL

La venue de l'utilisation massive d'outils personnels au travail, notamment les tablettes, les téléphones intelligents, les applications dans les navigateurs Web, etc. oblige les organismes à gérer ces types d'actifs informationnels.

L'utilisateur ne doit pas :

- Utiliser d'outils personnels au travail à des fins professionnelles sans avoir d'abord reçu l'autorisation du RSI.

7.5. MÉDIAS SOCIAUX

Les règles en vigueur dans l'établissement relatives à la *Politique du CHU de Québec sur l'utilisation des médias sociaux* (n^{o} 237-00) font partie intégrante de la présente politique.

7.6. UTILISATION DES ACTIFS INFORMATIONNELS POUR DES FINS SYNDICALES OU ASSOCIATIVES

Il est interdit d'utiliser les actifs informationnels de l'établissement à des fins syndicales ou associatives, et ce, sans qu'une entente formelle soit faite avec l'établissement.

7.7. UTILISATION DU TÉLÉTRAVAIL

Seules les personnes expressément autorisées par leur supérieur immédiat à utiliser le télétravail ont accès aux services ou aux logiciels qui leur seront explicitement autorisés par le RSI, selon des modalités précises. L'utilisateur doit respecter les ententes formelles de l'établissement et les directives qui en découlent afin d'assurer le respect de la présente politique.

7.8. PLAN DE CONTINUITÉ DES ACTIVITÉS

L'établissement doit élaborer un plan de continuité des activités (PCA) dans le but d'améliorer de façon proactive la résilience de l'établissement face à la perturbation de sa capacité à atteindre ses objectifs clés. L'établissement doit poursuivre la livraison de ses prestations de services à des niveaux acceptables et s'assurer que ces plans soient disponibles, connus, testés et utilisés par ses utilisateurs.

7.9. PLANS DE RELÈVE INFORMATIQUE

Le RSI doit s'assurer que les détenteurs des actifs informationnels ont planifié de tester, avec la collaboration de la Direction des ressources informationnelles (DRI), des plans de relève informatiques dans le but de s'assurer de la remise en opération des systèmes d'information essentiels en cas de panne majeure. De plus, des mesures de relève doivent être révisées et publiées annuellement.

7.10. PROJETS DE DÉVELOPPEMENT OU DE MODIFICATION DES SYSTÈMES D'INFORMATION

Le RSI ou les personnes qu'il délègue doivent définir les mesures de sécurité à mettre en place pour tout nouveau projet, et ce, dès la rédaction des analyses préliminaires.

7.11. ENTENTES ET CONTRATS

Toute entente ou tout contrat doit spécifier les exigences de l'établissement en matière de sécurité de l'information.

7.12. UTILISATION DES IMPRIMANTES ET DES TÉLÉCOPIEURS

Toute personne qui achemine ou imprime un document contenant des renseignements à caractère personnel et confidentiel doit en assurer la protection.

Les imprimantes et les télécopieurs doivent être placés de façon à éviter toute utilisation et observation non autorisée, soit dans un endroit surveillé et non accessible par le public.

7.13. GESTION DES INCIDENTS DE SÉCURITÉ INFORMATIONNELLE

Tout évènement indésirable touchant la sécurité de l'information doit être rapporté au RSI en respectant le processus de gestion des incidents en vigueur.

7.14. SENSIBILISATION ET FORMATION

L'établissement doit organiser sur une base régulière des activités de sensibilisation et de formation concernant la sécurité de l'information, et ce, dans le but de s'assurer d'une compréhension et d'une appropriation des objectifs de la présente politique.

7.15. ENGAGEMENT DE CONFIDENTIALITÉ

L'établissement fait signer un engagement de confidentialité par tous ses utilisateurs et ses tiers (*cf.* Annexe 1).

8. RÔLES ET RESPONSABILITÉS

La structure fonctionnelle de la sécurité de l'information de l'établissement ainsi que les rôles et responsabilités des principaux intervenants en sécurité de l'information sont décrits dans le *Cadre de gestion de la sécurité de l'information* (CGSI) de l'établissement. Celui-ci se conforme au Cadre de gestion de la sécurité de l'information de la Direction générale des technologies de l'information du ministère de la Santé et des Services sociaux. Malgré la description faite dans le document ci-haut mentionné, il faut souligner que :

- La présidente-directrice générale est l'ultime responsable de la sécurité des actifs informationnels. Le responsable de la sécurité de l'information (RSI), nommé par cette dernière, est responsable, notamment de planifier la mise en œuvre de la sécurité de l'information de son établissement. Tous les utilisateurs doivent respecter la présente politique.

9. AUTRES DISPOSITIONS

9.1. SANCTIONS

Lorsqu'un utilisateur contrevient ou déroge à la présente politique ou à tout document qui en découlent, il s'expose à :

- Des mesures disciplinaires et administratives ou toutes autres sanctions appropriées pouvant aller jusqu'au congédiement, conformément aux directives de l'établissement, aux règlements et aux conventions collectives de travail en vigueur;
- La révocation de certains droits d'accès aux équipements et services visés par la présente politique;
- Un remboursement à l'établissement de toutes sommes, y compris celles émanant d'un jugement prononcé par tout tribunal ou organisme réglementaire quelconque à l'endroit de l'établissement;

L'organisme s'engage à coopérer à toute requête provenant des forces de l'ordre ou à la demande de tout autre organisme mandaté à cet effet.

10. PROCÉDURE DÉCOULANT DE LA PRÉSENTE POLITIQUE

La procédure suivante découle de la présente politique :

- *Procédure concernant les règles d'utilisation des systèmes d'information du CHU de Québec*, n^{o} 271-30.1.

11. OUVRAGES CONSULTÉS

Les principaux ouvrages consultés sont présentés en Annexe 2.

12. MÉCANISMES DE RÉVISION

Le cas échéant, la présente politique et les documents qui l'accompagnent seront mis à jour à la suite de modifications apportées au *Cadre de gestion sur la sécurité de l'information*, à la *Politique provinciale de sécurité de l'information* ainsi qu'aux lois et règlements en vigueur, ou bien pour tenir compte des nouvelles pratiques et technologies utilisées au CHU de Québec-Université Laval ainsi que des besoins exprimés. Sinon, ils seront révisés au plus tard le 28 novembre 2020.

13. APPROBATION ET ENTRÉE EN VIGUEUR

La présente politique entre en vigueur le jour de son approbation par le conseil d'administration du CHU de Québec-Université Laval, soit le 28 novembre 2016.

Elle abroge et remplace la politique du CHU de Québec en matière de sécurité informationnelle précédemment approuvée par le Conseil d'administration le 10 février 2014.

CHU DE QUEBEC-UNIVERSITÉ LAVAL
Direction des technologies de l'information
(2016-11-01)
YF/hl

OBJET :	POLITIQUE DE SÉCURITÉ DE L'INFORMATION DU CHU DE QUÉBEC-UNIVERSITÉ LAVAL	POLITIQUE N^{O} 271-30

ANNEXES

- **ANNEXE 1 — Engagement au respect des mesures de sécurité de l'information et des exigences en matière de protection des renseignements personnels et des renseignements de santé et de services sociaux au CHU de Québec-Université Laval**
- **ANNEXE 2 — Ouvrages consultés**

ANNEXE 1

ENGAGEMENT AU RESPECT DES MESURES DE SÉCURITÉ DE L'INFORMATION ET DES EXIGENCES EN MATIÈRE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DES RENSEIGNEMENTS DE SANTÉ ET DE SERVICES SOCIAUX AU CHU DE QUÉBEC-UNIVERSITÉ LAVAL

Je, _____, exerce des activités au CHU de Québec-Université Laval (CHU) dans le cadre desquelles : - Je peux me voir octroyer des accès me permettant d'utiliser des actifs informationnels, logiciels ou autres outils technologiques; - Je peux avoir accès, créer, utiliser, communiquer, conserver ou détruire des renseignements personnels ou des renseignements de santé et de services sociaux.	☒
Je m'engage à prendre connaissance de l'ensemble des politiques ainsi que des codes de conduite, procédures et autres politiques encadrant l'utilisation sécuritaire des actifs informationnels, logiciels et autres outils technologiques du CHU et la protection des renseignements personnels et des renseignements de santé et de services sociaux, à y adhérer et à les respecter, lesquels me sont rendus accessibles sur l'intranet du CHU.	☒
Je dois en tout temps prendre toutes les mesures mises à ma disposition afin d'assurer la sécurité de l'information et la protection des renseignements personnels et des renseignements de santé et de services sociaux dans l'exercice de mes fonctions et des tâches qui y sont associées.	☒
J'ai le devoir d'informer sans délai mon supérieur immédiat et les instances identifiées à cet effet, de tout incident ou de toute situation portée à ma connaissance qui serait susceptible de compromettre la disponibilité, l'intégrité et la confidentialité des renseignements personnels et des renseignements de santé et de services sociaux ou de tout élément devant demeurer autrement confidentiel ainsi que concernant l'utilisation des actifs informationnels et de télécommunication.	☒
Je m'engage à ne jamais dévoiler des renseignements susceptibles de mettre en péril soit la confidentialité des renseignements confidentiels auxquels j'ai accès, soit la sécurité des actifs informationnels et de télécommunication de l'établissement.	☒
Je m'engage à ne pas utiliser les accès aux outils technologiques qui me sont octroyés par le CHU pour accéder à mes renseignements personnels ou renseignements de santé et services sociaux ou à des renseignements personnels ou renseignements de santé et services sociaux d'autres personnes en dehors du cours de mes fonctions (par ex. résultats d'examen d'un membre de la famille ou d'un proche, une consultation médicale d'un ami, le dossier d'un collègue, le dossier d'un usager à qui je n'offre pas de soins ou de services directement ou indirectement, etc.). Dans tous les cas, je dois limiter ma consultation des renseignements personnels et des renseignements de santé et de services sociaux à ceux qui sont nécessaires à l'exercice de mes fonctions ou activités au sein du CHU.	☒
Je suis avisé(e), informé(e) et conscient(e) que le CHU utilise des logiciels de sécurité qui enregistrent, pour des besoins de gestion, le contenu de mon courrier électronique, les adresses Internet des sites que je visite et conserve un dossier de toute activité réalisée sur ses réseaux d'information au cours de laquelle je transmets ou reçois quelque document que ce soit.	☒

ENGAGEMENT AU RESPECT DES MESURES DE SÉCURITÉ DE L'INFORMATION ET DES EXIGENCES EN MATIÈRE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DES RENSEIGNEMENTS DE SANTÉ ET DE SERVICES SOCIAUX AU CHU DE QUÉBEC-UNIVERSITÉ LAVAL

Je peux être soumis(e), de manière ponctuelle, à un audit ou à une vérification informatique, si requis. Ce faisant, je ne peux m'attendre à ce que ces utilisations aient un caractère privé ou confidentiel. J'ai été informé(e) également qu'il pourrait y avoir des mesures administratives ou disciplinaires prises à mon égard dans le cas où je manquerais à mes engagements.	☒
Je conserve le droit au respect de ma vie privée et de ma dignité lorsque j'œuvre au sein de l'établissement. Toutefois, cette protection est limitée. En effet, l'organisme a le droit de gérer, de se protéger, de protéger les usagers et d'obtenir des renseignements sur les utilisateurs de ses outils technologiques, et ce, à plus forte raison lorsqu'ils en sont avisés au préalable.	☒
Je suis informé(e) qu'Internet, le courrier électronique, l'intranet et les réseaux d'information de l'établissement sont mis à ma disposition pour une utilisation professionnelle, plus spécifiquement pour des tâches reliées à l'exercice de mes fonctions.	☒
Considérant que j'ai reçu l'autorisation d'accéder à distance aux applications de l'établissement (Cristal-Net/DPE ou autres), je m'engage à utiliser les renseignements fournis uniquement dans le cadre de mes fonctions au sein de l'établissement et exclusivement pour des usagers de l'établissement.	☒

ANNEXE 2

Principaux ouvrages consultés

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

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

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

QUÉBEC. *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ, P-39.1.

CANADA. *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C., (2000), c. 5.

CANADA. *Loi sur le droit d'auteur*, L.R.C., (1985) c. C-42.

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

QUÉBEC. *Loi sur les services préhospitaliers d'urgence*, RLRQ, c. S-6.2.

QUÉBEC. *Loi médicale*, RLRQ, c. M-9.

QUÉBEC. *Loi sur la pharmacie*, RLRQ, c. P-10.

QUÉBEC. *Loi sur la santé publique*, RLRQ, c. S-2.2.

QUÉBEC. *Loi sur la protection de la jeunesse*, RLRQ, c. P-34.1.

QUÉBEC. *Loi sur le curateur public*, RLRQ, c. C-81.

QUÉBEC. *Code des professions*, RLRQ, c. C-26, articles 60.4 à 60.6 et 87.

Codes de déontologie des différents ordres professionnels œuvrant dans le domaine de la santé et des services sociaux.

MSSS-POL01 Politique provinciale de sécurité de l'information, août 2015.

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

QUÉBEC. *Code civil du Québec*, RLRQ, c-CCQ-1991.

QUÉBEC. *Loi sur les archives*, RLRQ, c. A-21.1.

CANADA. *Loi canadienne sur les droits de la personne*, L.R.C. (1985), c. H-6.

CANADA. *Code criminel*, L.R.C. (1985) c. C-46.

CANADA. *Charte canadienne des droits et libertés de la personne.*

Politique du CHU de Québec en matière de sécurité informationnelle, nº 271-30, 2014.

Politique de sécurité de l'Institut universitaire en santé mentale de Québec, 2009.

Règlement 40 sur la gestion IUCPQ-Université Laval.