Centre intégré
de santé et de services
sociaux de Chaudière-
Appalaches
Québec

POLITIQUE

NUMÉRO : *POL_DRIGI_2017-118*

POLITIQUE DE SÉCURITÉ DE L'INFORMATION DU CISSS DE CHAUDIÈRE-APPALACHES

Préparé par : *La Direction des ressources informationnelles et de la gestion de l'information*	**Référence :** Politique provinciale de sécurité de l'information, Cadre de gestion de la sécurité de l'information et aux règles particulières émises par le ministère de la Santé et des Services sociaux.
Adoptée ou approuvée par : *Le conseil d'administration* *Résolution n^{o} 2017-13-15.*	**En vigueur le :** 22 mars 2017 **Révisée le :**

TABLE DES MATIÈRES

1. CONTEXTE

En 2015, le ministère de la Santé et des Services sociaux a ratifié une nouvelle politique provinciale et un cadre de gestion sur la sécurité de l'information. La Loi sur la santé et des services sociaux, qui détermine le rôle d'un organisme de santé, traite également de la sécurité des actifs informationnels (AI) puisque l'utilisation des technologies de l'information par les organismes de santé et des services sociaux est essentielle pour la réalisation de leurs missions. Par conséquent, l'utilisation de cette information doit être adéquate et faire l'objet d'une protection en lien avec sa valeur. L'organisme de santé reconnaît aussi détenir ou avoir sous sa responsabilité des renseignements personnels et confidentiels; ce qui exige une vigie rigoureuse de notre part puisque nous devons respecter plusieurs lois et règles particulières émises régulièrement.

Le CHU de Québec-Université Laval (CHU), le Centre intégré universitaire de santé et de services sociaux de la Capitale-Nationale (CIUSSS de la Capitale-Nationale), l'Institut universitaire de cardiologie et de pneumologie de Québec-Université Laval (IUCPQ) et le Centre intégré de santé et de services sociaux de Chaudière-Appalaches (CISSS-CA) ont collaboré pour rédiger cette politique. Cette collaboration a pour but, notamment, d'établir une approche semblable en matière de gestion de la sécurité de l'information. La principale raison qui a initié cette démarche est motivée par le partage régulier d'informations entre des intervenants issus de mêmes professions.

La présente politique est essentielle afin d'orienter l'organisme en matière de sécurité. Elle est le premier jalon d'un cadre de gestion de la sécurité de l'information. Elle établit notamment les mesures de sécurité logiques, physiques, humaines et organisationnelles à appliquer. De plus, elle détermine pour l'ensemble des utilisateurs, les comportements à adopter afin de s'assurer de l'utilisation appropriée de ses AI et de ses informations.

La protection des AI s'articule autour de cinq grands axes, à savoir :

- Disponibilité, intégrité, confidentialité, authentification et irrévocabilité (DICAI).

2. OBJECTIFS DE LA POLITIQUE

Cette politique de sécurité de l'information sert de principale fondation et permet à l'organisme d'assurer le respect des cinq grands axes (DICAI) tout au long du cycle de vie, de tous les AI détenus ou sous sa responsabilité.

La politique 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'organisme.
- La sécurité de l'information au regard de l'utilisation des réseaux informatiques des organismes, notamment l'Internet, l'infonuagique, le courrier électronique du Réseau intégré de télécommunication multimédia (RITM).
- La conformité aux lois et règlements applicables ainsi que les directives, normes et orientations gouvernementales.
- La mise en place d'une culture de sécurité de l'information particulièrement par la sensibilisation et la responsabilisation accrues des utilisateurs quant aux risques et enjeux entourant l'utilisation de l'information.

3. CHAMP D'APPLICATION

Cette politique s'applique à toute personne physique ou morale dûment autorisée à avoir accès aux AI détenus par l'organisme, peu importe l'endroit où elle se trouve ou la localisation de l'actif.

L'information visée par la politique est celle que l'organisme détient dans l'exercice de sa mission que sa conservation soit assurée par lui-même ou par un tiers.

4. DÉFINITIONS

Les définitions sont présentées à l'annexe 1 de la présente politique.

5. ÉNONCÉS ET PRINCIPES GÉNÉRAUX

Tout utilisateur au sein de l'organisation ayant accès à des informations assume des responsabilités en matière de sécurité; il doit respecter et appliquer les principes énoncés dans la politique et est redevable de ses actions auprès du président-directeur général de son organisme. Toute information générée par les utilisateurs est la propriété exclusive de l'organisme. Le principe du privilège d'accès minimal est appliqué en tout temps lors de l'attribution d'accès aux actifs informationnels.

La mise en œuvre et la gestion de la sécurité reposent sur une approche holistique. Cette approche tient compte des aspects humains, organisationnels, financiers, juridiques et techniques. Les mesures de protection, de prévention, de détection et de correction doivent assurer le DICAI des AI, de même que la continuité des activités. Elles doivent notamment prévenir les incidents, les erreurs, la malveillance ou la destruction d'information sans autorisation.

Une évaluation périodique des risques et des mesures de protection des AI doit être effectuée afin d'obtenir l'assurance qu'il y a adéquation entre les risques, les menaces et les mesures de protections déployées.

5.1. Protection des renseignements personnels et confidentiels

L'organisme reconnait qu'elle 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.

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'organisme. Toutefois, la protection à la vie privée ne limite pas les actions que l'organisme 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.

L'organisme utilise des outils de surveillance, de contrôle et d'enregistrement de toute utilisation de ses AI et peut en tout temps analyser et évaluer l'usage qui en est fait. Par conséquent, afin de permettre la détection de logiciels malveillants sans angle mort, l'organisme est autorisé à surveiller tout trafic transitant par ses réseaux informatiques incluant toutes les connexions encryptées. Ceci inclus, la surveillance des services courriels en ligne ainsi que tout autre service à usage personnel. Seuls, certains sites jugés de confiance absolue sont exempts de ce type d'audit.

5.1.1. Collecte

Il est interdit à tout utilisateur de recueillir un renseignement personnel ou confidentiel si cela 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.

5.1.2. Accès et utilisation

Les renseignements personnels ou confidentiels doivent être utilisés et ne servir qu'à des 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 doivent tenir un registre à cet effet. Toute personne qui utilise les AI de l'organisme mis à sa disposition doit s'assurer que tout document confidentiel, quel que soit son support, soit hors d'atteinte en le conservant en lieu sûr.

En plus des sanctions stipulées à l'article 7, le détenteur de l'information avec l'appui du RSI ou toute autre personne autorisée peut réviser, suspendre ou révoquer un privilège d'accès lorsque, entre autres raisons, l'utilisateur :

- 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'organisme.
- Termine son contrat ou son assignation.
- Quitte définitivement l'organisme ou est congédié.
- Divulgue des renseignements personnels ou confidentiels pour des raisons autres que celles prévues dans l'exercice de ses fonctions.
- Fais l'objet d'une suspension.

5.1.3. Communication

Tout utilisateur qui reçoit 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 informations concernant les usagers, que ce soit son propre dossier, celui d'un de ses proches ou toute autre personne. En cas de violation de cet engagement, l'organisme pourra imposer des sanctions disciplinaires ou administratives (voir art. 7 — sanctions).

Selon les balises prévues à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, certains renseignements peuvent ou doivent parfois être protégés et ne pas être accessibles aux citoyens. Il s'agit notamment de renseignements qui pourraient avoir une incidence économique, politique ou légale pour l'organisme. 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 et de l'article 17 de la Loi sur les services de santé et les services sociaux, l'usager a le droit de consulter son dossier ou d'en obtenir 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. Ces accès doivent être possibles quelle que soit la forme des documents : écrite, graphique, sonore, visuelle, informatisée ou autre.

5.1.4. Conservation et destruction

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

5.2. Utilisation d'internet, du RITM et des réseaux informatiques de l'organisme

Les AI sont mis à la disposition des utilisateurs par l'organisme 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 utilise 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 AI et de télécommunication, les outils Internet, le RITM incluant ses réseaux sans-fil qui sont accessibles à l'aide des réseaux informatiques de l'organisme, ne doivent pas être utilisés en violation des lois et réglementations en vigueur. De plus, l'organisme conformément aux lois et règlements, s'engage à coopérer face à toute requête en provenance des forces de l'ordre ou tout autre organisme mandaté à cet effet.

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 que les équipements informatiques portables de l'organisme (ex. tablette électronique, téléphone portable, ordinateur portable) qui sont la propriété de l'organisme pour communiquer avec le RITM.
- Utiliser les appareils personnels (ex. tablette, portable, téléphone intelligent, etc.) sur les réseaux de l'organisme lorsque le RSI leur en a donné l'autorisation à la suite d'une demande d'accès. L'organisme se réserve le droit de configurer ces équipements personnels afin de s'assurer de la sécurité de son réseau informatique et celui du RITM.
- Respecter la confidentialité de la connaissance partielle ou totale, de la structure des réseaux d'information de l'organisme. De plus, les utilisateurs doivent s'assurer que leur utilisation des réseaux d'information n'altère pas la structure de ceux-ci.

Enfin, l'organisme pourrait exiger qu'un utilisateur rembourse les frais de réparation ou autres frais encourus par l'organisme qui seraient reliés à une utilisation non autorisée, inadéquate ou malveillante dudit AI.

L'utilisateur ne doit pas :

- Afficher tout document ou tout 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'organisme.
- Profiter des facilités d'accès à Internet pour propager un virus sur les réseaux informatiques de l'organisme.
- Se servir des facilités d'accès à Internet ou au RITM ou tout autre moyen pour rendre inutilisable ou surcharger les ordinateurs et le réseau, ou pour contourner tout système mis en place pour protéger la vie privée ou la sécurité des AI ou des autres utilisateurs.
- Utiliser un modem sur un poste de travail sans l'approbation du RSI.
- N'installer ni modifier un actif informationnel sauf s'il en a eu l'autorisation 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 les personnes qu'il délègue, les utilisateurs peuvent conserver des documents sur des supports amovibles chiffrés (clé USB, disque dur externe).
- Emmagasiner en aucun cas des informations concernant un usager (photos, résultats de laboratoire, etc.) sur leurs AI personnels (portables, téléphones intelligents, infonuagique, clé USB, etc.).
- Divulguer la structure des réseaux d'information de l'organisme en tout ou en partie.

5.3. Utilisation du courrier électronique

Les règles en vigueur dans l'organisme relatives à l'utilisation du courrier électronique font partie intégrante de la présente politique.

Les utilisateurs qui ont 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'organisme. S'il s'agit d'un renseignement concernant un usager, l'utilisateur doit respecter les règles de tenue de dossiers de l'organisme. 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 n'ait préalablement été effectuée par le responsable de sécurité de l'information.

- 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.

Le formulaire de consentement ainsi que le formulaire de demande de projet pour l'évaluation des risques sont disponibles sur l'Intranet de l'organisme.

- 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.

5.4. Utilisation de la visioconférence

Les médecins ou les professionnels de la santé doivent utiliser la visioconférence supportée par les Réseaux universitaires intégrés de santé (RUIS), qui utilisent la plateforme RITM pour faire des consultations ou des suivis avec les usagers. C'est un environnement où la confidentialité des échanges est protégée.

Les applications du type Skype ou FaceTime par exemple n'assure pas la confidentialité des échanges. Règle générale, elles ne doivent pas être utilisées.

Dans l'éventualité où ce type de moyen est autorisé par le RSI, il doit être inscrit au plan de soin ou au plan d'intervention de la personne recevant des services comme moyen technologique pour soutenir l'intervention du médecin ou du professionnel.

Le consentement de l'usager ou de son représentant légal est obligatoire. De plus, l'usager doit être avisé des risques liés à l'utilisation de la visioconférence et des mesures de sécurité que l'organisation a mis en place pour les gérer.

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

5.6. Médias sociaux

Les règles en vigueur dans l'organisme relatives à la politique sur l'utilisation des médias sociaux se conforment à la présente politique.

5.7. Utilisation des actifs informationnels pour des fins syndicales ou associatives

Il est interdit d'utiliser les AI de l'organisme à des fins syndicales ou associatives sans qu'une entente formelle soit faite avec l'organisme.

5.8. L'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'organisme et les directives qui en découlent afin d'assurer le respect de la présente politique.

5.9. Plan de continuité des affaires

L'organisme doit élaborer un plan de continuité des affaires (PCA) afin d'améliorer de façon proactive la résilience de l'organisme face à la perturbation de sa capacité à atteindre ses objectifs clés. L'organisme 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.

5.10. Plan de relève informatique

Le RSI doit s'assurer que les détenteurs des AI ont planifié, avec la collaboration de la Direction des ressources informationnelles et de la gestion de l'information, des plans de relève informatique, les tester afin 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 annuellement.

5.11. Projet de développement ou de modification des systèmes d'informations

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.

5.12. Ententes et contrats

Toute entente ou tout contrat impliquant des AI doit spécifier les exigences de l'organisme en matière de sécurité de l'information.

5.13. 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 et configurés de façon à éviter toute utilisation ou observation non autorisée, soit dans un endroit surveillé et non accessible par le public.

5.14. 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, adopté sous le numéro : PROC-CDD2016-211.

5.15. Sensibilisation et formation

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

5.16. Engagement de confidentialité

L'organisme fait signer un engagement de confidentialité par tous ses utilisateurs et ses tiers.

6. RÔLES ET RESPONSABILITÉS

La structure fonctionnelle de la sécurité de l'information de l'organisme ainsi que les rôles et responsabilités des principaux intervenants en sécurité de l'information sont décrit s dans le cadre de gestion de la sécurité de l'information (CGSI) de l'organisme. Celui-ci se conforme au MSSS-CDG01 Cadre de gestion de la sécurité de l'information 2015-08-17 en vigueur du ministère de la Santé et des Services sociaux. Malgré la description faite dans le document ci-haut mentionné, il faut souligner que :

« Le président-directeur général est l'ultime responsable de la sécurité des actifs informationnels. Le RSI nommé par celui-ci est responsable, notamment, de planifier la mise en œuvre de la sécurité de l'information de son organisme. Tous les utilisateurs doivent respecter la présente politique ».

7. SANCTIONS

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

- Des mesures disciplinaires et administratives ou toutes autres sanctions appropriées conformément aux directives de l'organisme, aux règlements et aux conventions collectives de travail en vigueur.
- La révocation de certains droits d'accès aux équipements et services visés par cette politique.
- Un remboursement de toutes sommes à l'organisme. Cela inclut un jugement prononcé par tout tribunal ou organisme réglementaire quelconque.

8. ENTRÉE EN VIGUEUR

La présente politique entre en vigueur au moment de son adoption par le conseil d'administration de l'organisme.

9. RÉFÉRENCES

L'organisme s'est appuyé, notamment, sur la nouvelle politique provinciale de sécurité de l'information et son cadre de gestion d'août 2015 pour rédiger la présente politique. Les autres références se retrouvent à l'annexe 2.

10. MISE À JOUR DE LA POLITIQUE

La présente politique doit être révisée minimalement aux trois ans afin de s'assurer qu'elle est conforme aux lois, aux directives du ministère de la Santé et des Services sociaux et du Secrétariat du Conseil du trésor, aux nouvelles pratiques et aux technologies utilisées au sein de l'organisme.

Annexe 1 – Définitions

Actif informationnel : Actif informationnel au sens de la LPRS, soit, une banque d'information, un système d'information, un réseau de télécommunication, une infrastructure technologique ou un ensemble de ces éléments ainsi qu'une composante informatique d'un équipement médical spécialisé ou ultraspécialisé. Est également considéré comme un actif informationnel, tout support papier contenant de l'information.

Authentification : Acte permettant d'établir la validité de l'identité d'une personne ou d'un dispositif;

Authentifiant : Une information confidentielle détenue par une personne et permettant son authentification;

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

Confidentialité: Propriété d'une information de n'être accessible, ni divulguée qu'aux personnes ou entités désignées et autorisées.

Détenteur : Un employé désigné par son organisme public, 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;

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

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 concernant le droit d'auteur;

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

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.

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.

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

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.

Organisme : Ensemble des organismes qui relèvent du Dirigeant réseau de l'information (DRI) de la santé et des services sociaux en vertu de l'article 2, paragraphe 5 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LGGRI).

Périphérique : Dispositif matériel distinct de l'unité centrale de traitement d'un ordinateur, à laquelle il est relié, et qui peut assurer l'entrée ou la sortie de données.

Principe de moindre privilège ou privilège d'accès minimal : Une autorisation d'accès restreinte de manière à ce que l'utilisateur puisse n'accomplir avec celle-ci que les seules tâches autorisées et nécessaires à l'exercice de ses fonctions;

Renseignement confidentiel: donnée ou information désignée confidentielle par une loi, un règlement ou l'organisation à laquelle seules les personnes dûment autorisées peuvent avoir accès ou dont la communication la diffusion est limitée aux seules personnes ou entités dûment autorisées.

Renseignements personnels : Les renseignements qui concernent une personne physique et permettent 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 personne;

Réseau intégré de télécommunication multimédia (RITM) : C'est le principal véhicule d'échange d'information entre les organismes du réseau de la Santé et des Services sociaux.

Tiers : Toute personne morale ou physique qui exerce certaines fonctions hors mission à l'intérieur de l'organisme.

Usager : Toute personne qui utilise les services d'un organisme communautaire en santé et services sociaux, les services préhospitaliers d'urgence ou qui est hébergée dans une résidence privée pour aînés ou une ressource privée d'hébergement en dépendance relativement aux services qu'elle a reçu ou aurait dû recevoir;

Utilisateur : Toute personne physique ou morale, groupe ou entité administrative qui fait usage d'un ou de plusieurs AI sous la responsabilité de l'organisme. Notamment, les stagiaires, les résidents, les externes, les chercheurs, les médecins, le personnel et les bénévoles et les tiers, etc.

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.

Annexe2 – Références

Les principales références consultées sont :

- La Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, L.R.Q., c. G-1.03;
- La Loi concernant le cadre juridique des technologies et l'information, L.R.Q., c. C-1.1;
- La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, L.R.Q., c. A-2.1;
- La Loi sur la protection des renseignements personnels dans le secteur privé;
- La Loi sur la protection des renseignements personnels et les documents électroniques;
- La Loi sur le droit d'auteur, L.R., 1985, c. C-42;
- La Loi sur les services de santé et les services sociaux, L.R.Q., c. S-4.2;
- La Loi sur les services préhospitaliers d'urgence, L.R.Q, c. S-6.2;
- La Loi médicale, L.R.Q., c. M-9;
- La Loi sur la pharmacie, L.R.Q., c. P-10;
- La Loi sur la santé publique, L.R.Q., c. S-2.2;
- La Loi sur la protection de la jeunesse, L.R.Q., c. P-34.1;
- La Loi sur le curateur public, L.R.Q., c. C-81;
- Le Code des professions, L.R.Q., c. C-26, articles 60.4 à 60.6 et 87;
- Les 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 aout 2015
- La Charte des droits et libertés de la personne, L.R.Q., c. C-12;
- Le Code civil du Québec, L.Q., 1991, c. 64;
- La Loi sur les archives, L.R.Q., c. A-21.1;
- La Loi canadienne sur les droits de la personne, L.R., 1985, c. H-6;
- Le Code criminel, L.R., 1985, c. C-46;
- Charte canadienne des droits et libertés de la personne;
- Politique du CHU de Québec en matière de sécurité informationnelle, 2014
- Politique de sécurité de l'Institut universitaire en santé mentale de Québec, 2009
- Règlement 40 sur la gestion IUCPQ-Université Laval
- Politique de sécurité CISSS de Chaudière-Appalaches

Annexe 3 – Engagement à la politique

ENGAGEMENT DE CONFIDENTIALITÉ ET AU RESPECT DE LA POLITIQUE DE SÉCURITÉ DE L'INFORMATION DU CISSS DE CHAUDIÈRE-APPALACHES

Je_____, employé du Centre Intégré de santé et de services sociaux de Chaudière-Appalaches (CISSS de Chaudière-Appalaches) dont le siège social est situé au 363, route Cameron, Sainte-Marie (Québec) G6E 3E2, confirme avoir été informé de l'existence de la *Politique de sécurité de l'information de l'organisme* dont le texte intégral est disponible sur demande en format papier à la DRIGI, auprès de mon chef de service, sur l'intranet du CISSS de Chaudière-Appalaches sous l'onglet «Outil de travail - Règlements, politiques, procédures et protocoles».	☐ Cocher
Je m'engage à prendre connaissance de cette politique ainsi que des codes de conduite, procédures et autres politiques découlant de celle-ci, à y adhérer et à les respecter. Je dois en tout temps prendre toutes les mesures mises à ma disposition afin d'appliquer cette politique dans l'exercice de mes fonctions et des tâches qui y sont associées.	☐ Cocher
J'ai le devoir d'informer sans délai mon supérieur immédiat ou le responsable de la sécurité de l'information (RSI), 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 confidentiels et de l'utilisation des actifs informationnels et de télécommunication.	☐ Cocher
Je m'engage à ne jamais dévoiler des renseignements susceptibles de mettre en péril soit la confidentialité des renseignements et des données personnelles et confidentielles auxquels j'ai accès, soit la sécurité des actifs informationnels et de télécommunication de l'organisme.	☐ Cocher
Je suis pleinement conscient que le CISSS de Chaudière-Appalaches utilise des logiciels de sécurité qui enregistrent, pour des besoins de gestion, le contenu du courrier électronique organisationnel, 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 lorsque j'utilise les systèmes d'information et les ressources de l'organisme. Je peux être soumis de manière ponctuelle, à un audit ou à une vérification informatique si requis par le responsable de la sécurité de l'information (RSI) de l'organisme. J'ai été informé également qu'il pourrait y avoir des mesures administratives ou disciplinaires prises à mon égard dans le cas où je manquerais à mes engagements.	☐ Cocher
Je conserve le droit au respect de ma vie privée et de ma dignité lorsque j'œuvre au sein de l'organisme. Toutefois, cette protection est limitée. En effet, l'organisme a le droit de gérer, de se protéger, protéger ses usagers et d'obtenir des renseignements sur ses utilisateurs, et ce, à plus forte raison lorsqu'ils en sont avisés au préalable.	☐ Cocher
Je suis informé qu'Internet, le courrier électronique, l'intranet et les réseaux d'information de l'organisme sont mis à ma disposition pour une utilisation professionnelle, plus spécifiquement pour des tâches reliées à l'exercice de mes fonctions.	☐ Cocher
Je suis informé également que l'organisme a l'intention de surveiller lesdites utilisations et que, ce faisant, je ne peux m'attendre à ce que ces utilisations aient un caractère privé ou confidentiel. Les actifs informationnels et de télécommunication, les outils d'Internet ou tout autre outil de travail qui est accessible par les réseaux d'information de l'organisme ne doivent pas être en violation des lois et règlements en vigueur. Ces outils utilisés pour des activités illégales entraînent des mesures disciplinaires ou administratives. De plus, l'organisme s'engage conformément aux lois et règlements à coopérer face à toute requête en provenance des forces de l'ordre ou tout autre organisme mandaté à cet effet.	☐ Cocher
Considérant que j'ai reçu l'autorisation d'accéder à distance aux applications de l'organisme (DPE/DCI ou autres), je m'engage à utiliser les renseignements fournis uniquement dans le cadre de mes fonctions au sein de l'organisme et exclusivement pour des usagers de l'organisme.	☐ Cocher

ENGAGEMENT DE CONFIDENTIALITÉ ET AU RESPECT DE LA POLITIQUE DE SÉCURITÉ DE L'INFORMATION DU CISSS DE CHAUDIÈRE-APPALACHES PAR SES TIERS[i]

Je_____, du _____ dont le siège social est situé au _____, confirme avoir été informé de l'existence de la *Politique de sécurité de l'information de l'organisme* dont le texte intégral est disponible sur demande en format papier auprès de mon chef de service, sur l'intranet du CISSS de Chaudière-Appalaches sous l'onglet «Outil de travail - Règlements, politiques, procédures et protocoles».	☐ Cocher
Je m'engage à prendre connaissance de cette politique ainsi que des codes de conduite, procédures et autres politiques découlant de celle-ci, à y adhérer et à les respecter. Je dois en tout temps prendre toutes les mesures mises à ma disposition afin d'appliquer cette politique dans l'exercice de mes fonctions et des tâches qui y sont associées.	☐ Cocher
J'ai le devoir d'informer sans délai mon supérieur immédiat ou le responsable de la sécurité de l'information (RSI), 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 confidentiels et de l'utilisation des actifs informationnels et de télécommunication.	☐ Cocher
Je m'engage à ne jamais dévoiler des renseignements susceptibles de mettre en péril soit la confidentialité des renseignements et des données personnelles et confidentielles auxquels j'ai accès, soit la sécurité des actifs informationnels et de télécommunication de l'organisme.	☐ Cocher
Je suis pleinement conscient que le CISSS de Chaudière-Appalaches utilise des logiciels de sécurité qui enregistrent, pour des besoins de gestion, le contenu du courrier électronique organisationnel, 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 lorsque j'utilise les systèmes d'information et les ressources de l'organisme. Je peux être soumis de manière ponctuelle à un audit ou à une vérification informatique, si requis par le responsable de la sécurité de l'information (RSI) de l'organisme. J'ai été informé également qu'il pourrait y avoir des mesures administratives ou disciplinaires prises à mon égard dans le cas où je manquerais à mes engagements.	☐ Cocher
Je conserve le droit au respect de ma vie privée et de ma dignité lorsque j'œuvre au sein de l'organisme. Toutefois, cette protection est limitée. En effet, l'organisme a le droit de gérer, de se protéger, protéger ses usagers et d'obtenir des renseignements sur ses utilisateurs, et ce, à plus forte raison lorsqu'ils en sont avisés au préalable.	☐ Cocher
Je suis informé qu'Internet, le courrier électronique, l'intranet et les réseaux d'information de l'organisme sont mis à ma disposition pour une utilisation professionnelle, plus spécifiquement pour des tâches reliées à l'exercice de mes fonctions.	☐ Cocher
Je suis informé également que l'organisme a l'intention de surveiller lesdites utilisations et que, ce faisant, je ne peux m'attendre à ce que ces utilisations aient un caractère privé ou confidentiel. Les actifs informationnels et de télécommunication, les outils d'Internet ou tout autre outil de travail qui est accessible par les réseaux d'information de l'organisme ne doivent pas être en violation des lois et règlements en vigueur. Ces outils, utilisés pour des activités illégales, entraînent des mesures disciplinaires ou administratives. De plus, l'organisme s'engage conformément aux lois et règlements à coopérer face à toute requête en provenance des forces de l'ordre ou tout autre organisme mandaté à cet effet.	☐ Cocher

[i] **Tiers** : Toute personne morale ou physique qui exerce certaines fonctions hors mission à l'intérieur de l'organisme.