

<p>POL-12-314 Ancien numéro : POL_DRI_2017-118.B</p>	<p>Sécurité de l'information du CISSS de Chaudière-Appalaches</p>	
<p>Direction responsable : Direction des ressources informationnelles</p>		<p>En vigueur le : 22 mars 2017</p>
<p>Adoptée par : Le conseil d'administration Le comité de direction</p>		<p>Révisée le : 14 février 2024</p>
<p>Référence(s) : <i>Politique provinciale de sécurité de l'information</i> <i>Cadre provincial de gestion de la sécurité de l'information</i> <i>Règles particulières émises par le ministère de la Santé et des Services sociaux</i> <i>15 mesures obligatoires émises par le Secrétariat du Conseil du trésor (SCT)</i></p>		

TABLE DES MATIÈRES

1.	Contexte et définition.....	4
1.1.	Contexte.....	4
1.2.	Définition	4
2.	Principes.....	8
3.	Fondements légaux et éthiques	8
4.	Valeurs organisationnelles actualisées	9
5.	Objectifs	9
6.	Personnes visées	10
7.	Énoncé de politique.....	10
7.1.	Protection des renseignements personnels et confidentiels	10
7.2.	Gestion des accès et utilisation sécuritaire des actifs informationnels.....	11
7.2.1.	Demande d'accès	11
7.2.2.	Gestion des mots de passe.....	11
7.2.3.	Utilisation sécuritaire des actifs informationnels.....	12

7.2.4. Collecte	13
7.2.5. Communication	13
7.2.6. Classification, conservation et destruction	13
7.2.7. Utilisation du courrier électronique	13
7.2.8. Utilisation des outils collaboratifs (vidéoconférence).....	14
7.2.9. Utilisation des outils personnels au travail (BYOD).....	14
7.3. Télétravail.....	14
7.4. Internet.....	15
7.4.1. Les sites Web bloqués	15
7.4.2. Les médias sociaux.....	15
7.5. Gestion des périphériques	16
7.5.1. Utilisation des imprimantes et des télécopieurs	16
7.5.2. Disques durs externes, clés USB.....	16
7.6. La gestion des risques	16
7.6.1. Catégorisation des actifs informationnels.....	16
7.6.2. Analyse de risques.....	17
7.6.3. Analyse de préjudices	17
7.6.4. Analyse de sécurité technique	17
7.6.5. Test d'intrusion.....	17
7.6.6. Prime aux bogues	17
7.6.7. Évaluation des facteurs relatifs à la vie privée (EFVP).....	18
7.6.8. Gestion des incidents de sécurité	18
7.7. Sécurité physique.....	18
7.8. Gestion des vulnérabilités et des menaces	18
7.9. Sauvegarde et restauration	18
7.9.1. Plan de continuité des activités	18
7.9.2. Plan de relève informatique.....	19
7.10. Projet de développement ou de modification des systèmes d'information	19
7.10.1. Utilisation secondaire des données.....	20
7.11. L'intelligence artificielle.....	20
7.12. L'infonuagique.....	21
7.13. La transformation numérique	21
7.14. Les objets connectés.....	22
7.15. Cybersécurité	22
7.16. Ententes et contrats	22

7.17. Audit et conformité	22
7.18. Sensibilisation et formation	22
8. Responsabilités	23
9. Sanctions.....	23
10. Documents découlant de cette présente politique.....	23
11. Évaluation et révision	24
12. Références	24
Annexe I : Références	25
Annexe II : Engagements	26
Engagement à la Politique de sécurité de l'information du CISSS de Chaudière-Appalaches	26
Engagement à la Politique de sécurité de l'information du CISSS de Chaudière-Appalaches pour le personnel à haut privilege	27
Engagement à la Politique de sécurité de l'information du CISSS de Chaudière-Appalaches (tiers).....	28

1. Contexte et définition

1.1. Contexte

La présente politique de sécurité de l'information vise à établir des règles précises en matière de sécurité et de contrôle afin de protéger les renseignements personnels et confidentiels détenus par le Centre intégré de santé et de services sociaux de Chaudière-Appalaches (CISSS de Chaudière-Appalaches). Elle vise à répondre aux exigences émises dans la politique provinciale de sécurité de l'information MSSS-POL01 du 19 septembre 2022 et du cadre provincial de gestion de la sécurité de l'information MSSS-CDG01 du 9 janvier 2023. Celle-ci vient établir 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 actifs informationnels (AI) et de ses informations. La protection des actifs informationnels s'articule autour de cinq (5) grands axes, à savoir : disponibilité, intégrité, confidentialité, authentification et irrévocabilité (DICA). L'établissement s'est doté de cette politique afin de répondre à ses obligations et d'assurer une rigueur exemplaire concernant la sécurité de l'information.

1.2. Définition

Actif informationnel

Banque d'informations, 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.

Appareil mobile

Appareil pouvant être déplacé tels : les téléphones cellulaires, les téléphones intelligents, les ordinateurs portables, les tablettes électroniques dotés de la technologie "Bluetooth" qui permet d'accéder à Internet.

Authentification

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

Authentifian

Une information confidentielle détenue par une personne et permettant son authentification.

Bluetooth

Norme de communications permettant l'échange bidirectionnel de données à très courte distance en utilisation des ondes radio. Son objectif est de simplifier les connexions des liaisons filaires.

CERTAQ

C'est une équipe de travail du ministère de la Cybersécurité et du Numérique qui s'occupe de coordonner les incidents de cybersécurité.

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.

Courrier électronique

Le courrier électronique est un service très utilisé sur Internet. Il permet à un expéditeur d'envoyer un message à un ou plusieurs destinataires.

Confidentialité

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

Cyberdéfense

Ensemble des mesures techniques et non techniques permettant à un État de défendre, dans le cyberspace, les systèmes d'information jugés essentiels.

Cybersécurité

La cybersécurité est définie comme la protection de l'information numérique et de l'infrastructure sur laquelle elle repose. C'est un ensemble d'outils et de processus de sécurité visant à protéger les réseaux, les ordinateurs et les données. La cybersécurité est gérée par des professionnels formés pour faire face spécifiquement aux menaces persistantes avancées. En revanche, la sécurité de l'information pose les bases de la sécurité des données et forme les professionnels à prioriser les ressources avant d'éliminer les menaces ou les attaques.

Cycle de vie de l'information

L'ensemble des étapes que franchit une information et qui vont de sa création, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction, en conformité avec le calendrier de conservation de l'organisation.

Détenteur de l'information

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 entourant de cette information ainsi que celle 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 sur le droit d'auteur (L.R.C. (1985), c. C-42).

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 ou plusieurs événements liés à la sécurité de l'information, indésirables ou inattendus, présentant une probabilité forte de compromettre les opérations liées à l'activité de l'établissement et de menacer la sécurité de l'information (disponibilité, intégrité ou confidentialité). Un incident de sécurité de l'information peut être lié ou non à l'utilisation des technologies de l'information et des communications.

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.

Intelligence artificielle

Ensemble de technologies visant à simuler l'intelligence humaine et ses processus cognitifs dans l'apprentissage, le raisonnement, la compréhension des langues naturelles ou encore la perception de l'environnement.

Objets connectés

Interconnexion entre Internet et des objets, des lieux et des environnements physiques. Cette connexion permet une communication entre nos biens et des existences numériques (ex. : pompes à insuline, moniteur cardiaque, serrures de porte, chauffage intelligent, etc.).

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.

NIST

Le National Institute of Standards and Technology (NIST). Le NIST est une agence gouvernementale américaine chargée d'élaborer et de promouvoir des normes, des mesures et des technologies afin d'améliorer la sécurité et la compétitivité économique du pays. Le NIST travaille dans des domaines tels que les technologies de l'information, la cybersécurité, la métrologie, l'ingénierie, la fabrication et la science des matériaux. Il est également chargé de créer et de maintenir des normes et des lignes directrices dans des domaines tels que la cryptographie, la sécurité de l'information et la protection de la vie privée. Le NIST est une organisation très importante pour la promotion de l'innovation et du développement technologique aux États-Unis.

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.

Plan de continuité des activités

Plan contenant les rôles et responsabilités définis des personnes et des équipes ayant autorité pendant et après un incident. Ce plan détaille les informations permettant de gérer les conséquences immédiates d'un incident perturbateur.

Plan de reprise informatique (PRI)

Procédures coordonnées pour récupérer et mettre à jour des opérations critiques, probablement sur un site alternatif, en cas d'urgence, de défaillance du système ou de désastre, le temps de rétablir les opérations normales sur le site primaire. Ces activités informatiques mettent en œuvre l'ensemble des processus et des moyens humains, matériels et technologiques permettant à l'organisation de faire face à un sinistre.

Principe du moindre privilège ou privilège d'accès

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 auxquelles seules les personnes dûment autorisées peuvent avoir accès ou dont la communication, la diffusion est limitée aux seules personnes ou entités dûment autorisées.

Renseignement personnel

Renseignement qui concerne 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 personne.

Réseau intégré de télécommunication multimédia (RITM)

C'est le principal véhicule d'échange d'informations 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'établissement.

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 reçus ou aurait dû recevoir.

Utilisateur

Toute personne physique ou morale, groupe ou entité administrative qui fait usage d'un ou de plusieurs actifs informationnels sous la responsabilité du CISSS de Chaudière-Appalaches. Notamment, les stagiaires, les résidents, les externes, les chercheurs, les médecins, le personnel, les bénévoles et les tiers (fournisseurs, partenaires, etc.), 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 système lui servant à leur tour de moyen de propagation et qui produit les actions malveillantes pour lesquelles il a été conçu.

2. Principes

Le CISSS de Chaudière-Appalaches reconnaît que :

- Tout utilisateur au sein de l'établissement ayant accès à des informations assume des responsabilités en matière de sécurité de l'information; il doit respecter et appliquer les principes énoncés dans la politique et est redevable de ses actions auprès du président-directeur général de son établissement;
- Toute information générée par les utilisateurs est la propriété exclusive de l'établissement. Le principe du moindre privilège d'accès est appliqué en tout temps lors de l'attribution d'accès aux actifs informationnels;
- La mise en œuvre et la gestion de la sécurité de l'information 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 la disponibilité, l'intégrité, la confidentialité, l'authentification et l'irrévocabilité des actifs informationnels, de même que la continuité des activités. Elles doivent notamment prévenir les incidents, les erreurs, la malveillance ou la destruction d'information sans autorisation;
- Qu'une évaluation périodique des risques et des mesures de protection des actifs informationnels soit effectuée afin d'obtenir l'assurance qu'il y a adéquation entre les risques, les menaces et les mesures de protection déployées;
- Qu'il 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;
- 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.

3. Fondements légaux et éthiques

Cette politique fait partie du cadre de gestion du CISSS de Chaudière-Appalaches et s'y inscrit, sans s'y limiter, en conformité avec :

- La Loi modifiant la Loi sur la gouvernance du MSSS des ressources informationnelles des organismes publics et des entreprises du gouvernement (LQ 2021, chapitre 22)¹;
- La Directive gouvernementale sur la sécurité de l'information (2021)²;

¹ [LQ 2021, c 22 | Loi modifiant la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement et d'autres dispositions législatives | CanLII](#)

- Le Cadre provincial de gestion de la sécurité de l'information (2023-01-09)³;
- La Politique provinciale de gestion de la sécurité de l'information (2022-09-19)⁴;
- ISO/IEC 27005-2022 Gestion des risques liés à la sécurité de l'information (2022-10);
- Décret 596-2020 Programme de consolidation des centres de traitement informatique (CTI).

4. Valeurs organisationnelles actualisées

La sécurité de l'information est d'une importance capitale pour notre établissement. Nous reconnaissons que la protection des données de nos usagers, de nos partenaires et de notre personnel est essentielle pour garantir la crédibilité du CISSS de Chaudière-Appalaches.

Cette politique vise à définir les valeurs fondamentales qui guident ns efforts en matière de sécurité de l'information.

Nous déployons l'énergie nécessaire afin de nous assurer que la disponibilité, l'intégrité et la confidentialité des données soient respectées.

En adhérant à ces valeurs, nous nous engageons à maintenir un environnement sécurisé et fiable, renforçant ainsi la confiance de nos parties prenantes et assurant le succès à long terme de notre établissement au niveau de la sécurité de l'information.

5. Objectifs

Cette politique de sécurité de l'information sert de fondement et permet à l'établissement d'assurer le respect des cinq (5) grands axes (DICA) tout au long du cycle de vie, de tous les actifs informationnels détenus ou sous sa responsabilité. La politique permet :

- De protéger les informations sensibles et les données confidentielles de l'établissement contre les menaces internes et externes, telles que les cyberattaques, les fuites de données et les vols;
- D'accéder aux informations essentielles quand elles sont nécessaires, en minimisant les interruptions de service dues à des pannes matérielles, des erreurs humaines ou des attaques (**disponibilité**);
- De s'assurer que les informations restent intactes et non altérées. Ce qui implique de détecter et de prévenir les modifications non autorisées des données (**intégrité**);
- D'autoriser aux seules personnes les accès aux informations sensibles, en mettant en place des mécanismes d'authentification, de chiffrement et de contrôle d'accès (**confidentialité**);
- De s'assurer d'un processus existant permettant l'(**authentification et identification**) d'une personne avant de lui donner accès aux actifs informationnels (code d'utilisateur, mot de passe, questions d'identification);
- De s'assurer qu'il soit impossible de nier qu'une opération, un transfert ou une transaction ait eu lieu (journalisation, certificat, conservation, etc.);
- De se conformer aux lois, réglementations et normes pertinentes en matière de sécurité de l'information;
- De sensibiliser et permettre de renseigner les employés à la sécurité de l'information, afin de réduire les risques liés à des erreurs humaines ou à une mauvaise utilisation des informations;
- D'avoir un regard sur l'utilisation de ses réseaux informatiques, notamment l'Internet, l'infonuagique, le courrier électronique du Réseau intégré de télécommunication multimédia (RITM);

² [Directive gouvernementale sur la sécurité de l'information](#)

³ [Cadre gouvernemental de gestion; Sécurité de l'information](#)

⁴ [Politique provinciale de gestion de la SI: \(rtss.qc.ca\)](#)

- D'identifier, évaluer et atténuer les risques potentiels pour la sécurité de l'information, en mettant en place des mesures de sécurité appropriées;
- D'élaborer une saine gestion des incidents de sécurité et d'atténuer les risques potentiels ainsi que répondre adéquatement aux incidents de sécurité;
- D'auditer et d'évaluer les mécanismes de sécurité mis en place;
- De planifier et mettre en œuvre des stratégies pour assurer la continuité des activités en cas de perturbation majeure (plans de reprise informatique);
- D'instaurer une démarche d'amélioration continue de la sécurité de l'information en tenant compte des évolutions technologiques et des menaces émergentes;
- De mettre en place une culture de cybersécurité et 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 et ainsi d'accroître leur connaissance sur les menaces cybernétiques dont sont confrontés les établissements de santé.

6. Personnes visées

Cette politique s'applique à toute personne physique ou morale (les employés, médecins, résidents, stagiaires, tiers) dûment autorisée à avoir accès aux actifs informationnels (AI) détenus par le CISSS de Chaudière-Appalaches, peu importe l'endroit où ils se trouvent ou sa localisation et le support sur lequel ils se trouvent durant tout leur cycle de vie, c'est-à-dire de leur collecte ou de leur création jusqu'à leur versement aux archives.

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

- La signature de l'engagement à la politique de sécurité de l'information implique l'acceptation de cette politique. Un refus de signature entraîne un retrait des accès.

7. Énoncé de politique

7.1. Protection des renseignements personnels et confidentiels

La nouvelle *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, LQ 2021, c 25 adoptée le 21 septembre 2021 actualise l'encadrement applicable à la protection des renseignements personnels dans diverses lois, dont en ce qui concerne le CISSS de Chaudière-Appalaches, elle vient modifier :

- La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels⁵;
- La Loi sur l'assurance maladie 1999, c. 89 a. 42⁶;
- La Loi concernant le cadre juridique des technologies de l'information C-1.1⁷;
- La Loi concernant le partage de certains renseignements de santé P-9.0001⁸;
- La Loi sur les services de santé et les services sociaux S-4.2⁹;
- La Loi sur les services de santé et les services sociaux pour les autochtones cris S-5¹⁰.

⁵ La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels

⁶ [A-29 - Loi sur l'assurance maladie \(gouv.qc.ca\)](#)

⁷ [C-1.1 - Loi concernant le cadre juridique des technologies de l'information \(gouv.qc.ca\)](#)

⁸ [P-9.0001 - Loi concernant le partage de certains renseignements de santé \(gouv.qc.ca\)](#)

⁹ [S-4.2 - Loi sur les services de santé et les services sociaux \(gouv.qc.ca\)](#)

Elle précise diverses exigences relatives au consentement requis préalablement à une collecte, une utilisation ou une communication de renseignement personnel. *Elle prescrit que le consentement nécessaire à certaines utilisations ou communications d'un renseignement personnel sensible doit être manifesté de façon expresse.*

Pour plus d'informations, se référer au bureau de la protection des renseignements personnels de la Direction de la qualité, de l'évaluation, de la performance et de l'éthique.

7.2. Gestion des accès et utilisation sécuritaire des actifs informationnels

7.2.1. Demande d'accès

Un utilisateur ne peut effectuer une demande afin de s'octroyer à lui-même des accès dans les systèmes d'information, répertoires, etc. Le supérieur immédiat ou son délégué doit effectuer une demande d'accès pour son employé.

L'utilisation des données doit être encadrée par une bonne gestion des accès. Le principe du moindre privilège doit être basé sur le besoin réel de chaque utilisateur :

- 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. Lors de l'utilisation d'un poste authentifié par un compte générique, l'utilisateur doit ouvrir une session Citrix pour accéder à Internet avec son propre code et mot de passe.

Consultez la *Politique sur la gestion des accès logiques aux actifs informationnels du CISSS de Chaudière-Appalaches*.

7.2.2. Gestion des mots de passe

À partir des règles du NIST¹¹, le CISSS de Chaudière-Appalaches a établi les règles suivantes :

- Choisir un mot de passe complexe et, si le système le permet, à douze (12) caractères. La phrase de passe est fortement recommandée lorsque le système le permet (Monchienestunbergerde10ans). Cela rend les mots de passe plus faciles à retenir et potentiellement plus sécurés;
- Les systèmes d'information ne doivent pas contenir des comptes génériques. Un compte générique est permis pour l'ouverture de session uniquement après une analyse effectuée par la DRI;
- L'exigence d'expiration périodique des mots de passe est annuelle, sauf en cas de suspicion de compromission du compte. Cette recommandation repose sur le principe que les utilisateurs sont plus susceptibles de choisir des mots de passe forts s'ils n'ont pas à les changer fréquemment;
 - L'authentification multifactorielle (MFA) est à privilégier afin de renforcer les comptes des utilisateurs sur les sites exposés sur Internet.

¹⁰ [S-5 - Loi sur les services de santé et les services sociaux pour les autochtones cris \(gouv.qc.ca\)](#)

¹¹ Le National Institute of Standards and Technology (NIST) des États-Unis a publié des directives en matière de gestion des mots de passe, notamment dans le document NIST Special Publication 800-63B, intitulé « Digital Identity Guidelines. »

7.2.3. Utilisation sécuritaire des actifs informationnels

Les actifs informationnels sont mis à la disposition des utilisateurs par l'établissement 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 actifs informationnels, les outils Internet, le Réseau intégré de télécommunication multimédia (RITM) incluant ses réseaux sans-fil qui sont accessibles à l'aide des réseaux informatiques de l'établissement, ne doivent pas être utilisés en violation des lois et réglementations en vigueur. De plus, l'établissement, 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 équipements informatiques portables de l'établissement (ex. : tablette électronique, téléphone portable, ordinateur portable) qui sont la propriété de l'établissement pour communiquer avec le 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, le CISSS de Chaudière-Appalaches pourrait exiger qu'un utilisateur rembourse 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.

L'utilisateur ne doit pas :

- Utiliser les appareils personnels (ex. : tablette, portable, téléphone intelligent, etc.) sur le réseau médico-administratif de l'établissement (réseau filaire). Le réseau sans-fil public est par contre autorisé;
- Utiliser les appareils personnels à des fins personnelles pendant les heures de travail;
- Installer ni modifier un actif informationnel, sauf s'il en a eu l'autorisation par le Chef de la sécurité de l'information organisationnelle (CSIO) ou son désigné;
- Utiliser des périphériques externes pour conserver des documents. Exceptionnellement, avec l'autorisation du CSIO ou les personnes qu'il délègue, les utilisateurs peuvent conserver des documents sur des supports amovibles détenant une technologie de chiffrement. Les outils offerts dans Microsoft 365 sont à privilégier;
- Emmagasinier en aucun cas des informations concernant des usagers (photos, résultats de laboratoire, etc.) sur leurs appareils personnels (portable, téléphone intelligent, infonuagique, etc.).

Règles d'utilisation des systèmes d'information, vous référer à *DIR-DRI_2021-315 Directive sur les règles d'utilisation des systèmes d'information*.

Procédure sur les appareils mobiles *PRO-DRI_2022-302*

En plus des sanctions stipulées à l'article 9, le détenteur de l'information, avec l'appui du CSIO 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;
- Fait l'objet d'une suspension.

7.2.4. 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 25*, notamment en matière de consentement des usagers.

7.2.5. 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'établissement pourra imposer des sanctions disciplinaires ou administratives (voir art. 9 - Sanctions). *La loi modernisant des dispositions législatives en matière de protection des renseignements personnels* précise des sanctions selon les circonstances.

7.2.6. Classification, 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 ainsi que les procédures qui les accompagnent, la structure de classification et le calendrier de conservation est disponible auprès de la Direction de la qualité, de l'évaluation, de la performance et de l'éthique (DQEPE) de l'établissement.

Classification, conservation et destruction du dossier de l'utilisateur

Toute information concernant les usagers est gérée par les archives médicales de la Direction des services multidisciplinaires (DSM).

Pour plus d'informations au sujet des données des usagers et leur dossier, se référer à la *Procédure de gestion du dossier des usagers*.

7.2.7. Utilisation du courrier électronique

Les utilisateurs qui ont des privilèges d'accès au courrier électronique organisationnel doivent l'utiliser uniquement pour des raisons professionnelles :

- Toutes les personnes qui utilisent un autre courrier électronique (ex. : Université Laval) ne doivent pas transférer d'informations confidentielles appartenant à l'établissement (ex. : données sur les usagers). Le courrier électronique de l'établissement doit être utilisé à ces fins.

Pour plus d'informations sur l'utilisation du courrier électronique, se référer à la procédure sur l'utilisation du courrier électronique.

7.2.8. Utilisation des outils collaboratifs (vidéoconférence)

Les facilités offertes par la suite Microsoft 365 ne remplacent toutefois pas les systèmes de mission de l'établissement. L'information qui transige par les outils collaboratifs doit tout de même être intégrée, lorsque pertinente, dans ces systèmes (ex. : dossier de l'utilisateur).

La suite Microsoft 365 permet de partager de manière sécurisée les applications et les services corporatifs avec des utilisateurs invités, partenaires externes issus de n'importe quelle organisation. Toutefois, cette pratique doit répondre aux exigences de sécurité suivantes :

- L'utilisateur invitant doit s'assurer de l'identification de son invité;
- L'utilisateur invitant doit informer son invité de la sensibilité des échanges par les outils collaboratifs et les règles de sécurité à observer;
- L'utilisateur invitant doit veiller au respect des exigences de sécurité de son invité (capture d'écran, enregistrement, etc.);
- L'utilisateur invitant doit retirer le compte de son invité, dès que sa collaboration n'est plus requise ou à la suite du non-respect des règles de sécurité communiquées.

Le ministère de la Santé et des Services sociaux (MSSS) demande aux utilisateurs de la suite Microsoft 365 d'insérer une photo de profil, le représentant, permettant ainsi à ses interlocuteurs de mieux l'identifier. Cependant, ce choix de photo de profil doit correspondre à l'esprit de neutralité, d'intégrité et de sobriété, régissant la fonction publique et parapublique québécoise. Il est donc interdit d'utiliser des avatars, logos ou autres images, contraires à cet esprit. Il est plutôt suggéré d'utiliser une photo récente représentant l'utilisateur, avec un arrière-plan neutre.

Les médecins, résidents-médecins ou autres professionnels de la santé doivent utiliser la vidéoconférence 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.

L'outil collaboratif disposé à la vidéoconférence est :

- Teams;
- Tout autre outil déjà approuvé par le CSIO.

Les applications du type « Messenger » ou « FaceTime » n'assurent pas la confidentialité des échanges et sont interdites.

Le consentement de l'utilisateur ou de son représentant légal est obligatoire. De plus, l'utilisateur doit être avisé des risques associés à l'utilisation des moyens de communication.

Veillez-vous référer à la procédure relative à l'utilisation des applications de vidéoconférence.

7.2.9. Utilisation des outils personnels au travail (BYOD)

La venue de l'utilisation massive d'outils personnels au travail, notamment : les tablettes, les téléphones intelligents, les applications dans les navigateurs Web, etc. obligent les établissements à gérer ces types d'actifs informationnels (Réf 7.2.3).

Veillez-vous référer à la procédure sur les appareils mobiles.

7.3. 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 la Direction des ressources informationnelles, 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.

Politique sur la gestion du télétravail de la DRH

Directive sur le travail à distance

Les ordinateurs personnels sont acceptés en télétravail en utilisant la connexion FortiClient, Citrix Cloud ou GlobalProtect.

- Ces appareils doivent être munis d'un logiciel antivirus;
- Ces appareils doivent s'assurer de recevoir les mises à jour de sécurité sur une base régulière (ex. : mises à jour mensuelles de Windows, MacOS, etc.);
- Ces appareils ne peuvent pas utiliser une version de système d'exploitation obsolète qui n'a plus de possibilité de maintenir à jour (ex. : en date de mai 2022 : Windows 7, MacOS 10.14, Android 9, iOS11);
- Ces appareils ne peuvent pas accéder à toutes les ressources internes de la même façon qu'un appareil de l'entreprise. Après la connexion au VPN, les communications seront restreintes à certains protocoles tels :
- L'accès à des bureaux virtuels Citrix;
- L'accès aux communications téléphoniques Cisco Jabber;
- Certains sites Web sécurisés (ex. : Octopus Web);
- Il ne serait pas possible par exemple d'accéder à un partage de fichiers directement;
- Le CISSS de Chaudière-Appalaches se réserve le droit de modifier ou restreindre les accès de manière évolutive pour ces appareils en cas de risque de sécurité.

7.4. Internet

7.4.1. Les sites Web bloqués

Le CISSS de Chaudière-Appalaches se doit d'informer et de responsabiliser les utilisateurs et d'encadrer l'utilisation d'Internet.

Considérant la popularité de certains sites Web (comme la catégorie des médias sociaux, par exemple : X (anciennement Twitter), Facebook, YouTube, LinkedIn, etc.), le CISSS de Chaudière-Appalaches a écrit une directive sur le sujet. Vous pouvez la consulter dans l'intranet de l'établissement.

Le MSSS et le CISSS de Chaudière-Appalaches bloquent certains sites Web soit à connotation suspecte, à risque au niveau de la sécurité ou encore des sites jugés inappropriés, par exemple : pornographie, drogues, terroriste, sites de vente d'armes, sites haineux, hameçonnage, etc.

Directive sur les règles d'utilisation des systèmes d'information

7.4.2. Les médias sociaux

Pour ce qui est des demandes par les utilisateurs afin d'accéder aux sites des « médias sociaux », elles sont analysées par l'équipe de sécurité avant de donner l'accès.

Toute demande pour créer un compte Facebook organisationnel¹² doit être effectuée par Octopus et la DRI procédera à une vérification auprès du service des communications. Une fois l'approbation donnée par les communications, la DRI donnera accès au demandeur.

Directive sur l'utilisation des médias sociaux par toutes les personnes œuvrant au CISSS de Chaudière-Appalaches

7.5. Gestion des périphériques

7.5.1. 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 **inaccessible** par le public.
- Lorsqu'il est impossible de trouver un endroit adéquat, l'impression doit être sécurisée par un mécanisme (carte à puce) pour effectuer l'impression.
- L'impression sur un lieu de télétravail n'est pas permise par l'établissement.

Politique sur la gestion du télétravail

7.5.2. Disques durs externes, clés USB

Les clés USB, bien qu'inoffensives à première vue, sont l'une des principales causes de contamination par un virus et elles peuvent provoquer des préjudices importants pour le CISSS de Chaudière-Appalaches. Le simple fait d'insérer une clé USB dans un ordinateur de l'établissement peut mettre en péril le réseau informatique.

D'autres méthodes de transfert sont maintenant disponibles, soit :

- Courriel chiffré;
- OneDrive de Microsoft (celui inclus dans Microsoft 365);
- Nextcloud de l'établissement (pour des dossiers lourds et confidentiels à partager avec l'externe du RSSS);
- Teams.

7.6. La gestion des risques

7.6.1. Catégorisation des actifs informationnels

Le processus de catégorisation de l'information est un exercice permettant d'évaluer le degré de sensibilité et de criticité de son information. Cela permet d'attribuer un niveau d'impact à un actif informationnel pour chacun des critères de sécurité, à savoir : la disponibilité, l'intégrité et la confidentialité (DIC). Le résultat de cet exercice conditionne les mesures de sécurité à mettre en place.

¹² Compte Facebook créé par le service des communications ayant un nom représentatif d'un service faisant partie de l'établissement.

7.6.2. Analyse de risques

La protection de l'information revêt une importance capitale sur le plan gouvernemental. Une gestion des risques de sécurité de l'information permet :

- D'améliorer la sécurité de l'information;
- D'identifier, de gérer et de communiquer les risques de sécurité de l'information et leurs conséquences sur le fonctionnement de l'établissement;
- De se conformer aux exigences gouvernementales en sécurité de l'information, ainsi que celles véhiculées dans le cadre normatif ministériel;
- D'informer les détenteurs de l'état des systèmes quant à la protection qu'ils procurent à l'information grâce aux analyses de risques.

La gestion des risques de sécurité de l'information est un processus en collaboration avec le détenteur et son équipe (fiduciaire, pilote, etc.). Elle est définie par la norme ISO/CEI 27005 comme un ensemble d'activités coordonnées visant à diriger et piloter le CISSS de Chaudière-Appalaches vis-à-vis du risque. Les analyses de risque cibleront les actifs informationnels ayant une criticité élevée ou ayant une portée gouvernementale.

7.6.3. Analyse de préjudices

Par le Décret 596-2020, le gouvernement édicte la consolidation des centres de traitement informatique en mettant à profit les services infonuagiques. Dans un souci d'assurer la sécurité de l'information dans cette importante transformation, Infrastructures technologiques Québec (ITQ) s'est inspiré des travaux du gouvernement fédéral pour élaborer une méthodologie d'analyse de préjudices visant à déterminer la sensibilité de l'information et le type de services infonuagiques en capacité d'accueillir cette information.

Des ateliers sont effectués entre l'assistant cadre au Chef de la sécurité de l'information organisationnelle (CCSIO) de la DRI et le fiduciaire du domaine d'affaires et toutes autres personnes requises pour la réussite de cette analyse. L'ordonnancement de ces analyses s'effectuera dans l'ordre suivant :

- Systèmes déjà hébergés en service infonuagique;
- Nouveau système de basse criticité (CAT 1-2);
- Migration de systèmes de basse criticité (CAT 1-2)
- Nouveaux systèmes critiques ou rehaussement d'un système en place (CAT 3-4);
- Migration des systèmes critiques (CAT 3-4).

7.6.4. Analyse de sécurité technique

Lors de soumission pour de nouveaux produits, système biomédical ou autres, une analyse de sécurité est effectuée sur le système et le fournisseur de service.

7.6.5. Test d'intrusion

Suite aux analyses précédentes, pour certains actifs informationnels, un fournisseur peut se voir demander un test d'intrusion effectué par le Centre opérationnel de cybersécurité (COCD) afin de s'assurer de la sécurité de son produit.

7.6.6. Prime aux bogues

Suite aux analyses précédentes, si un actif informationnel est accessible à partir d'Internet, le site Web du fournisseur sera déclaré au ministère de la Cybersécurité et du Numérique (MCN) afin que son site Web soit scruté par des experts, et ce, pour éviter que le site contienne des défauts de conception ou autres anomalies.

7.6.7. Évaluation des facteurs relatifs à la vie privée (EFVP)

Cette évaluation est analysée par l'équipe responsable de la protection des renseignements personnels de la DQEPE. Cette évaluation permet de veiller au respect de la vie privée. La Loi 25 mentionne à l'article 63.5.

Évaluation des facteurs relatifs à la vie privée.

Consulter le bureau de protection des renseignements personnels du CISSS de Chaudière-Appalaches, par courriel : bureau.prp.ciSSsca@ssss.gouv.qc.ca

7.6.8. Gestion des incidents de sécurité

La gestion des incidents de sécurité de l'information est un processus obligatoire pour tous les organismes du réseau de la santé et des services sociaux. Il respecte la directive « MSSS-DIR01_Declaration-Incidents-Securite_v1-0 » entérinée le 17 août 2015 par le sous-ministre associé à la Direction générale des technologies de l'information du MSSS.

Le but de cette gestion des incidents de sécurité est de rétablir le fonctionnement normal d'un processus ou d'un service aussi rapidement que possible.

Afin d'en apprendre plus sur la déclaration d'incident de sécurité et sa gestion, veuillez consulter :

Procédure de gestion des incidents de sécurité de l'information;

Procédure sur la gestion des incidents de confidentialité impliquant un renseignement personnel.

7.7. Sécurité physique

La sécurité physique des salles de serveurs et de télécommunications est gérée par la Direction des ressources informationnelles (DRI). Ces salles sont sécurisées et non identifiées afin d'en prévenir l'intérêt des passants. Un contrôle d'accès strict est en place ainsi qu'une surveillance assidue.

7.8. Gestion des vulnérabilités et des menaces

Dans les quinze (15) mesures de sécurité obligatoires, un processus de détection des vulnérabilités est en place. Les correctifs doivent être appliqués selon l'importance de la vulnérabilité indiquée par le CERTAQ.

7.9. Sauvegarde et restauration

La règle particulière du MSSS¹³ mentionne la section sur la gestion de l'exploitation de s'assurer que les mesures de sécurité identifiées, notamment ceux assurant la sauvegarde, la surveillance et disponibilité des services, soient appliquées, effectives et efficaces.

La DRI possède un guide sur la sauvegarde, la rétention et la destruction des journaux qui encadre ce volet.

7.9.1. Plan de continuité des activités

L'établissement doit élaborer et mettre en place un plan de continuité des activités afin d'améliorer de façon proactive la résilience de l'établissement face à la perturbation de sa capacité à atteindre ses objectifs clés.

¹³ [RP-Securite-organisationnelle.aspx \(rtss.qc.ca\)](#)

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.

Les détenteurs doivent rédiger et tenir à jour leur plan de continuité des activités. Un plan de continuité des activités comprend les rôles et responsabilités des acteurs impliqués dans le plan, le processus d'activation, les détails permettant de gérer les conséquences immédiates d'un incident perturbateur en tenant compte du bien-être des individus, des options stratégiques, tactiques et opérationnelles et la prévention de toute perte d'indisponibilité d'activités prioritaires¹⁴.

Étapes d'un plan de continuité des activités

Il est essentiel de comprendre la structure de l'établissement et les actifs informationnels clés qu'elle détient :

- Identification des processus d'affaires critiques;
- Identification des technologies supportant les processus d'affaires;
- Élaboration et sélection des scénarios de risque;
- Conception du plan de continuité;
- Implantation;
- Tests et plan, formation et communication;
- Surveillance, mesure analyse et évaluation;
- Revue de direction;
- Amélioration continue.

7.9.2. Plan de relève informatique

Le CSIO doit s'assurer que les détenteurs des actifs informationnels ont planifié, avec la collaboration de la Direction des ressources informationnelles, des plans de relève informatique, de 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 si le système d'information a subi des changements au niveau de la disponibilité, l'intégrité et la confidentialité (DIC).

7.10. Projet de développement ou de modification des systèmes d'information

Le Chef de la sécurité de l'information organisationnelle (CSIO) 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. La catégorisation du système d'information, que ce soit en acquisition ou en développement par le CISSS de Chaudière-Appalaches, doit être réalisée avec la collaboration de l'assistant cadre au Chef de la sécurité de l'information organisationnelle (ACCSIO) et une ou plusieurs personnes ciblées par le détenteur de l'information.

Les applications acquises ou développées doivent être protégées contre les vulnérabilités dues à des failles dans les logiciels développés et qui rendent les organisations vulnérables, et ce, tout au long du cycle de vie de ces applications.

Une approche systématique basée sur l'amélioration de la sécurité applicative a démontré que la mise en place d'un modèle de développement sécurisé assurait une protection plus grande durant tout le cycle de vie de l'application et de meilleures pratiques dans l'ensemble de l'organisation.

¹⁴ ISO 22301 Gestion de la continuité des affaires.

Ce modèle repose donc sur la mise en place de processus, de règles, de procédures, de documentation, de sélection de contrôles de sécurité (aussi connus sous le nom de mesures de sécurité), de vérification, de tests, d'audit et de vigie technologique afin de s'assurer que la protection demeure efficace et adéquate de bout en bout.

C'est ce que propose la norme ISO 27034 et, en se basant sur cette norme, le CISSS de Chaudière-Appalaches contribue à l'amélioration de la gestion de la sécurité de ses informations par une intégration systématique de ses façons de faire dès la conception de l'application, et ce, tout au long de son existence caractérisée par les activités d'exploitation, de maintenance, de support, et ce, durant tout le cycle de vie de l'application. Cette discipline offre une assurance de maintenir un standard de qualité vérifiable et une sécurité mesurable en termes de conformité, de coûts, d'efficacité et de robustesse.

Pour une demande de développement (PowerApp ou autres), veuillez communiquer avec la DRI.

Pour une demande de développement (Power BI), veuillez communiquer avec la DQEPE.

7.10.1. Utilisation secondaire des données

Certains systèmes sont développés par des chercheurs universitaires de la Direction de la recherche et de l'enseignement universitaire, par l'équipe en analyse d'affaires de la Direction de la qualité, de l'évaluation, de la performance et de l'éthique et les autres directions pour leur propre domaine d'affaires, et ce, afin de contribuer à l'amélioration de la qualité, de l'efficacité et de la sécurité des soins ou encore à des fins statistiques.

Ces entrepôts sont alimentés par les systèmes sources et ont une grande valeur aux yeux de certaines personnes malveillantes (cybercriminels).

Afin de détecter les enjeux possibles, les entrepôts de données au CISSS de Chaudière-Appalaches doivent être approuvés par le développeur de cette base de données, la DQEPE et le Chef de la sécurité de l'information organisationnelle (CSIO) de la DRI.

Plusieurs volets sont à vérifier :

- Équité (aucune discrimination);
- Volet juridique (en cas d'erreur, à qui revient la responsabilité);
- La protection des renseignements personnels;
- Inclusivité (accessible à tous);
- Éthique (respect des valeurs morales).

7.11. L'intelligence artificielle

Plusieurs organisations font appel à l'intelligence artificielle (IA) pour optimiser leurs processus, analyser les données, assurer le diagnostic et le traitement de patients et personnaliser l'expérience de leurs utilisateurs.

L'intelligence artificielle transforme les façons de faire, cette technologie en développement fait appel à des programmes informatiques intelligents. On emploie l'IA pour effectuer des tâches particulières, comme utiliser la reconnaissance faciale pour accéder à votre appareil mobile par exemple ou demander à votre haut-parleur intelligent quelles sont les prévisions météorologiques.

Les auteurs de menace peuvent concevoir automatiquement des attaques par harponnage plus fréquentes et faire appel à un degré plus élevé de sophistication. Des courriels d'hameçonnage ou des messages d'escroquerie très réalistes pourraient mener à des vols d'identité, de la fraude financière ou à d'autres formes de cybercrimes.

Faites preuve de vigilance

L'intelligence artificielle est une technologie qui appartient au domaine de l'apprentissage automatique plutôt qu'à celui du véritable « renseignement ». Elle ne comprend pas les concepts, mais produit du contenu correspondant à la meilleure réponse possible d'un point de vue statistique afin de l'utiliser dans une requête.

N'oubliez pas :

- Il est important que l'utilisateur soit conscient que les résultats peuvent être erronés, non éclairés, illogiques ou faussés;
- Ne pas inclure des informations personnelles et confidentielles dans vos requêtes.

Comme cette technologie est de plus en plus utilisée et exploitée, il est probable qu'elle mène à une augmentation du nombre de cyberattaques sophistiquées, ce qui comprend l'hameçonnage, le piratage psychologique, la mésinformation, la désinformation et le vol d'identité.

Mesures d'atténuation des risques :

- Ne pas insérer d'informations personnelles ou confidentielles dans ces outils;
- Mettre en place des mécanismes d'authentification rigoureux (MFA);
- Appliquer les correctifs de sécurité et les mises à jour;
- Rester à l'affût des dernières menaces et vulnérabilités liées à l'IA;
- Journaliser vos actifs informationnels;
- Sensibiliser le personnel sur les attaques de piratage psychologique;
- Déclarer tout incident ou comportement inhabituel dans vos actifs informationnels.

7.12. L'infonuagique

Le ministère de la Cybersécurité et du Numérique (MCN) mentionne dans sa politique du 22 juillet 2022 que :

« La stratégie de transformation numérique du MSSS et du RSSS permettra à terme de bonifier la prestation de services aux citoyens. Elle constitue une opportunité, mais suscite également des préoccupations majeures à considérer en lien avec la protection de l'information sensible (médicale, psychosociale, etc.) détenue par ces entités. »

Le personnel du CISSS de Chaudière-Appalaches doit contacter la Direction des ressources informationnelles avant d'accepter ou de développer tout système d'information qui est hébergé dans un infonuagique. L'analyse de préjudice doit être réalisée en amont d'une nouvelle implantation ou mise à jour d'un système déjà en place.

La DRI pourra s'assurer de fournir le service d'infonuagique nécessaire et sécurisé pour la mise en place de tout nouveau système.

7.13. La transformation numérique

Le gouvernement du Québec a confié au ministère de la Cybersécurité et du Numérique (MCN) le mandat de faciliter la transformation numérique globale au sein de l'appareil public. Le Centre québécois d'excellence numérique (CQEN) a été créé afin de soutenir et conseiller les organismes publics dans leur transformation numérique. Ce changement vient impacter toutes les sphères de travail. Il est donc important de prévoir des arrangements importants avec les différents processus à améliorer ainsi qu'avec les solutions numériques sur lesquelles ils vont s'appuyer. Il est important de noter que la transformation numérique est

un processus complexe qui peut prendre du temps et nécessiter un engagement de la part des tous les utilisateurs du CISSS de Chaudière-Appalaches.

7.14. Les objets connectés

Le milieu de la santé ne passe pas à côté des objets connectés. L'utilisation des données numériques nous renvoie donc directement à ces données récoltées et emmagasinées par ces objets.

Tout appareil (biomédical ou autres) connecté au réseau du CISSS de Chaudière-Appalaches doit faire l'objet d'une analyse de sécurité par la Direction des ressources informationnelles afin de s'assurer que des contrôles de sécurité sont en place, et ce, afin de prévenir des incidents de nature technique et de protection des renseignements personnels (analyse de sécurité, 7.6.4).

Les objets connectés seront sécurisés dans un réseau différent du médico-administratif étant donné que les mises à jour de ces appareils ne suivent pas toujours la technologie de dernière pointe.

7.15. Cybersécurité

Le Secrétariat du Conseil du trésor a mis sur pied en 2019 une [politique gouvernementale de cybersécurité](#). C'est en conformité avec la transformation numérique gouvernementale et sur la base des acquis et des réalisations de l'administration gouvernementale en matière de cybersécurité que s'inscrit cette dite politique. Elle s'adresse aux organisations publiques, à leur personnel ainsi qu'à la population.

7.16. Ententes et contrats

Toute entente ou tout contrat impliquant des actifs informationnels doit spécifier les exigences de l'établissement en matière de sécurité de l'information. La Direction des ressources informationnelles doit être consultée afin qu'elle puisse donner les contrôles de sécurité adéquats.

7.17. Audit et conformité

La surveillance d'un réseau informatique est essentielle pour garantir son bon fonctionnement, sa sécurité et sa performance. La surveillance constitue une base solide pour un audit. Le but est d'en reconnaître les vulnérabilités, d'améliorer les performances et de garantir une expérience positive aux utilisateurs.

Chaque détenteur est responsable des audits reliés à leurs systèmes d'information. Cette tâche d'audit est attribuée au pilote du système.

7.18. Sensibilisation et formation

L'établissement 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.

La collaboration de toutes les directions est essentielle à la réussite des connaissances acquises par le personnel sous sa responsabilité.

Des formations sont disponibles à tous les utilisateurs :

- Cybersécurité – Mission possible (ENA1916) « obligatoire à la demande du Secrétariat du Conseil du trésor (SCT) »;
- Les menaces numériques : La sécurité des appareils mobiles « obligatoire à la demande du SCT »;

- Programme de sensibilisation en sécurité informationnelle.

Le site de l'ENA est accessible à cette adresse : <https://fcp.rtss.qc.ca/my/>

8. Responsabilités

La structure fonctionnelle de la sécurité de l'information du CISSS de Chaudière-Appalaches ainsi que les rôles et responsabilités des principaux intervenants en sécurité de l'information au CISSS de Chaudière-Appalaches sont décrits dans le « [Cadre provincial de gestion de la sécurité de l'information MSSS-CDG01 du 09 janvier 2023](#) ». Malgré la description faite dans le document ci-dessus mentionné, il faut souligner que :

« Le président-directeur général est l'ultime responsable de la sécurité des actifs informationnels. Le Chef de la sécurité de l'information organisationnelle (CSIO) est nommé par celui-ci et 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 ».

9. Sanctions

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

- Des mesures disciplinaires et administratives ou toutes autres sanctions appropriées 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 cette politique;
- Un remboursement de toutes sommes à l'établissement. Cela inclut un jugement prononcé par tout tribunal ou organisme réglementaire quelconque.

La Direction des ressources informationnelles collabore avec la Direction des ressources humaines pour toute demande d'enquête. Le gestionnaire doit faire une demande à son agent de gestion du personnel des relations de travail (AGP) et ce dernier contactera l'équipe de la sécurité de l'information, au besoin.

10. Documents découlant de cette présente politique

- Cadre de gestion de la sécurité de l'information du CISSS de Chaudière-Appalaches;
- Directive sur les règles d'utilisation des systèmes d'information;
- Directive sur le télétravail;
- Procédure relative au courrier électronique;
- Procédure relative à l'utilisation des applications de vidéoconférence;
- Procédure sur la gestion des incidents de sécurité;
- Procédure sur la catégorisation des systèmes d'information.

11. Évaluation et révision

Cette politique doit être révisée aux trois (3) ans ou avant afin de s'assurer qu'elle est conforme aux lois, aux directives du ministère de la Santé et des Services sociaux, du ministère de la Cybersécurité et du Numérique et du Secrétariat du Conseil du trésor, aux nouvelles pratiques et normes de sécurité et aux technologies utilisées au sein de l'établissement.

La présente politique entre en vigueur au moment de son adoption par le Comité de direction du CISSS de Chaudière-Appalaches.

12. Références

L'établissement s'est appuyé, notamment, sur la politique provinciale de sécurité de l'information et son cadre de gestion de septembre 2022 ainsi qu'à la politique gouvernementale de cybersécurité du Secrétariat du Conseil du trésor et la directive sur la cybersécurité MSSS-DIR03 du 20 novembre 2023 pour rédiger la présente politique. Les autres références se retrouvent à l'annexe 2.

HISTORIQUE DES VERSIONS (du plus ancien au plus récent)	
Numéro et titre	Date de révision
POL_DRI_2017-118.B Politique de sécurité de l'information du CISSS de Chaudière-Appalaches	14 février 2024

Annexe I : Références

Politique et autres documents du SCT, MSSS et du MCN :

- MSSS-POL01 Politique provinciale de sécurité de l'information;
- MSSS-CDG01 Cadre de gestion de la sécurité de l'information;
- Directive sur la cybersécurité;
- Règle particulière sur la sécurité organisationnelle.

Les lois, chartes et codes :

- La Loi modifiant la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, LQ 2021, chapitre 22;
- Loi sur les renseignements de santé et de services sociaux;
- La Loi concernant le cadre juridique des technologies de 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 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;
- 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;
- La Charte des droits et libertés de la personne, L.R.Q., c. C -12;
- Charte canadienne des droits et libertés de la personne;
- Le Code des professions, L.R.Q., c. C -26, articles 60.4 à 60.6 et 87;
- Le Code civil du Québec, L.Q., 1991, c. 64;
- Le Code criminel, L.R., 1985, c. C -46;

Divers sites consultés :

- <https://www.sciencepresse.qc.ca/baladodiffusion/2020/02/19/intelligence-artificielle-secours-soins-sante>
 - Barbara Decelle, conseillère à la recherche en santé chez IVADO – l'Institut de valorisation des données. Son mandat est de réunir les experts en recherche sur la santé et en science des données;
 - Cécile Petitgand, postdoctorante, Centre de recherche du Centre hospitalier universitaire de l'Université de Montréal (CRCHUM) et du Centre de recherche en droit public. Elle analyse l'implantation des outils d'intelligence artificielle dans les centres hospitaliers universitaires du Québec.
- <https://www.cairn.info/revue-pouvoirs-2019-3-page-5.htm#>
- <https://cdn.ey.com/echannel/fr/Industries/ey-barometre-de-maturite-de-l-ia-dans-les-chu.pdf>
- <https://theconversation.com/lia-dans-les-hopitaux-un-monde-entre-promesses-et-realite-132294>
- [dcpia-defrvp-fra.pdf](#)
- [Programme de consolidation des CTI - Québec \(gouv.qc.ca\)](#)
- [Le modèle DICAI - Securisa inc.](#)
- [Intelligence Artificielle - ITSAP.00.040 - Centre canadien pour la cybersécurité](#)
- [Programme de consolidation des CTI - Québec \(gouv.qc.ca\)](#)

Annexe II : Engagements

Engagement à la Politique de sécurité de l'information du CISSS de Chaudière-Appalaches

Je _____, œuvrant au CISSS de Chaudière-Appalaches, dont le siège social est situé au 363, route Cameron, Sainte-Marie (Québec) G6E 3E2, confirme avoir reçu l'information de l'existence de la <i>Politique relative à la sécurité de l'information du CISSS de Chaudière-Appalaches</i> , dont le texte intégral est disponible sur l'intranet de l'établissement, dans la section <i>Directions, ressources informationnelles, sécurité de l'information</i> .	<input type="checkbox"/> 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.	<input type="checkbox"/> Cocher
J'ai le devoir d'informer sans délai mon supérieur immédiat ou le Chef de la sécurité de l'information organisationnelle (CSIO) à l'adresse suivante : incident.securiteinformatique.cisssca@ssss.gouv.qc.ca ou par Octopus de tout incident ou de toute situation portée à ma connaissance qui seraient susceptibles de compromettre la disponibilité, l'intégrité et la confidentialité des renseignements confidentiels ainsi que concernant l'utilisation des actifs informationnels et de télécommunications.	<input type="checkbox"/> 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 télécommunications de l'établissement.	<input type="checkbox"/> Cocher
Je suis en pleine conscience que le CISSS de Chaudière-Appalaches utilise des logiciels de sécurité qui enregistrent, pour des besoins de gestion, le contenu de mon courrier électronique de l'organisation, les adresses Internet des sites que je visite quand je suis sur le réseau du CISSS de Chaudière-Appalaches, 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. On peut me soumettre, de manière ponctuelle, à un audit ou à une vérification informatique, si requis par le CSIO de l'établissement. Ce faisant, je ne peux m'attendre à ce que ces utilisations aient un caractère privé ou confidentiel. J'ai aussi reçu l'information qu'il pourrait y avoir des mesures administratives ou disciplinaires prises à mon égard dans le cas où je manquerais à mes engagements.	<input type="checkbox"/> Cocher
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'établissement a le droit 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.	<input type="checkbox"/> Cocher
J'ai reçu l'information 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.	<input type="checkbox"/> Cocher
Considérant que j'ai reçu l'autorisation d'accéder à distance aux applications de l'établissement (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 qui sont en lien avec ma clientèle.	<input type="checkbox"/> Cocher

**Engagement à la Politique de sécurité de l'information
du CISSS de Chaudière-Appalaches pour le personnel à haut privilege**

<p>Je _____, œuvrant au CISSS de Chaudière-Appalaches, dont le siège social est situé au 363, route Cameron, Sainte-Marie (Québec) G6E 3E2, confirme avoir reçu l'information de l'existence de la <i>Politique relative à la sécurité de l'information du CISSS de Chaudière-Appalaches</i> dont le texte intégral est disponible sur l'intranet du CISSS de Chaudière-Appalaches, dans la section <i>Règlements, politiques, procédures, protocoles et processus</i> sous l'onglet <i>Outils de travail</i>.</p>	<input type="checkbox"/> Cocher
<p>Je m'engage à prendre connaissance de la <i>Politique relative à la sécurité de l'information du CISSS de Chaudière-Appalaches</i> 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.</p>	<input type="checkbox"/> Cocher
<p>J'ai le devoir d'informer, sans délai, mon supérieur immédiat ou le Chef de la sécurité de l'information organisationnelle (CSIO) à l'adresse suivante : incident.securiteinformatique.ciSSsca@sSSS.gouv.qc.ca ou par Octopus de tout incident ou de toute situation portée à ma connaissance qui seraient susceptibles de compromettre la disponibilité, l'intégrité et la confidentialité des renseignements confidentiels ainsi que concernant l'utilisation des actifs informationnels et de télécommunications.</p>	<input type="checkbox"/> Cocher
<p>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 télécommunications de l'établissement. Je m'engage également à ne jamais dévoiler des renseignements confidentiels sur les affaires du CISSS de Chaudière-Appalaches contenus dans tout programme informatique, dans tout logiciel ou dans tout autre matériel de quelque nature que ce soit, fourni par l'établissement ainsi que toute rédaction de textes conçue pour lesdits programmes.</p>	<input type="checkbox"/> Cocher
<p>Je m'engage à ne jamais communiquer, transmettre, exploiter ou autrement faire usage, pour mon propre compte ou pour autrui, des informations contenues au CISSS de Chaudière-Appalaches. Je m'engage également à ne jamais reproduire, ni utiliser l'information confidentielle pour fabriquer, vendre, faire fabriquer ou faire vendre des produits ou technologies commercialisables, à moins d'en avoir reçu la permission de la Direction générale.</p>	<input type="checkbox"/> Cocher
<p>Je suis en pleine conscience qu'il m'est interdit d'utiliser mes privilèges sur des programmes utilitaires afin de contourner les mesures de sécurité des systèmes du CISSS de Chaudière-Appalaches.</p>	<input type="checkbox"/> Cocher
<p>Je m'engage à obtenir l'autorisation du CSIO ou de la personne qu'il désigne avant de procéder à un test de sécurité ou à tout autre test pouvant influencer le bon fonctionnement des applications ou des réseaux d'information. Je m'engage également à utiliser des données fictives ou anonymisées au moment de la formation des utilisateurs, lors de démonstrations de systèmes ou pour effectuer les tests requis. Dans l'impossibilité d'utiliser des données fictives, le personnel de la Direction des ressources informationnelles doit faire une demande officielle au CSIO ou à la personne qu'il désigne.</p>	<input type="checkbox"/> Cocher
<p>Je suis en pleine conscience que le CISSS de Chaudière-Appalaches 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 quand je suis sur le réseau du CISSS-CA 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. On peut me soumettre, de manière ponctuelle, à un audit ou à une vérification informatique, si requis par le CSIO de l'établissement. Ce faisant, je ne peux m'attendre à ce que ces utilisations aient un caractère privé ou confidentiel. J'ai aussi reçu l'information qu'il pourrait y avoir des mesures administratives ou disciplinaires prises à mon égard dans le cas où je manquerais à mes engagements.</p>	<input type="checkbox"/> Cocher
<p>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'établissement a le droit 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.</p>	<input type="checkbox"/> Cocher

Engagement à la Politique de sécurité de l'information du CISSS de Chaudière-Appalaches (tiers¹⁵)

Je _____, œuvrant au CISSS de Chaudière-Appalaches à titre de « tiers », dont le siège social est situé au 363, route Cameron, Sainte-Marie (Québec) G6E 3E2, confirme avoir reçu l'information de l'existence de la <i>Politique de sécurité de l'information du CISSS de Chaudière-Appalaches</i> , dont le texte intégral est disponible sur l'intranet du CISSS de Chaudière-Appalaches dans la section Directions, Ressources informationnelles, sécurité de l'information .	<input type="checkbox"/> 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.	<input type="checkbox"/> Cocher
J'ai le devoir d'informer sans délai le Chef de la sécurité de l'information organisationnelle (CSIO) à l'adresse suivante : incident.securiteinformatique.ciassca@ssss.gouv.qc.ca de tout incident ou de toute situation portée à ma connaissance qui seraient susceptibles de compromettre la disponibilité, l'intégrité et la confidentialité des renseignements confidentiels ainsi que concernant l'utilisation des actifs informationnels et de télécommunications.	<input type="checkbox"/> 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 télécommunications de l'établissement.	<input type="checkbox"/> Cocher
Je m'engage à m'informer des règles du CISSS de Chaudière-Appalaches pour tout transfert de renseignements obtenus de cet établissement, afin d'utiliser le meilleur outil sécuritaire et disponible.	<input type="checkbox"/> Cocher
Je suis en pleine conscience que le CISSS de Chaudière-Appalaches utilise des logiciels de sécurité qui enregistrent, pour des besoins de gestion, le contenu de mon courrier électronique de l'établissement uniquement , les adresses Internet des sites que je visite quand je suis sur le réseau du CISSS de Chaudière-Appalaches 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. On peut me soumettre, de manière ponctuelle, à un audit ou à une vérification informatique, si requis par le CSIO de l'établissement. Ce faisant, je ne peux m'attendre à ce que ces utilisations aient un caractère privé ou confidentiel. J'ai aussi reçu l'information qu'il pourrait y avoir des mesures administratives ou disciplinaires prises à mon égard dans le cas où je manquerais à mes engagements.	<input type="checkbox"/> Cocher
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'établissement a le droit 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.	<input type="checkbox"/> Cocher
J'ai reçu l'information qu'Internet, le courrier électronique de l'établissement , l'intranet et les réseaux d'information du CISSS de Chaudière-Appalaches sont mis à ma disposition pour une utilisation professionnelle, plus spécifiquement pour des tâches reliées à l'exercice de mes fonctions.	<input type="checkbox"/> Cocher
Je respecterai le présent engagement de confidentialité et de respect de la sécurité de l'information pendant toute la durée de mon affectation et, en tout temps, après la fin de celui-ci.	<input type="checkbox"/> Cocher
J'ai reçu l'information qu'en défaut de respecter tout ou en partie le présent engagement de confidentialité, je m'expose ou expose mon employeur à des recours légaux, des réclamations, des poursuites et toute autre procédure en raison du préjudice causé pour quiconque est concerné par le présent engagement.	<input type="checkbox"/> Cocher
Je confirme avoir lu les termes du présent engagement et en avoir saisi toute la portée.	<input type="checkbox"/> Cocher

Signature : _____ Date : _____

¹⁵ **Tiers** : Toute personne morale ou physique qui exerce certaines fonctions hors mission à l'intérieur de l'organisme