Centre intégré
de santé
et de services sociaux
des Laurentides
Québec

Politique

Titre	**Politique sur la sécurité de l'information**	
N°	**POL 2020 DQEPE 03**	
En vigueur	2020-10-21	
Révision	Ne s'applique pas	
Adoption	2020-10-21	Conseil d'administration du CISSS des Laurentides Résolution : R1037 2020.10.21
Approbation	2020-09-25	Comité de direction du CISSS des Laurentides
Validation	2019-12-02 2020-07-31	Comité sécurité de l'information des Laurentides Directeurs CISSS des Laurentides
Diffusion	2020-10-28	Dépôt sur l'intranet du CISSS des Laurentides
Responsable de l'application	Responsable de la sécurité de l'information - RSI (DQEPE)	
Application et personnes concernées	Toute personne contribuant à la mission du CISSS des Laurentides et toute autre personne qui exerce ou développe sa profession au sein de l'établissement	
Document(s) remplacé(s)	Politique de sécurité de l'information POL 2016 DPACQ 078	
Document(s) initiateur(s)	▪ Cadre de gestion de la sécurité de l'information MSSS-CDG01 ▪ Cadre de référence gestion de l'information CISSS Laurentides ▪ Politique de sécurité de l'information 2016 CISSS Laurentides	
Document(s) en découlant	▪ Cadre de gestion de la sécurité de l'information CISSS ▪ Tous les documents permettant d'encadrer la sécurité de l'information au CISSS des Laurentides	

Table des matières

N.B. Le genre masculin est utilisé comme générique,
dans le seul but de ne pas alourdir le texte.

1. Préambule

Dans le cadre de sa mission, le CISSS des Laurentides détient des informations sensibles concernant les citoyens, le personnel et la gestion de l'organisation. Ces informations sont quotidiennement manipulées par les utilisateurs (employés, médecins et autres) et en conséquence exposées à différents risques. Le CISSS des Laurentides ne fait aucun compromis quant à la sécurité de ses informations.

La présente politique ainsi que les documents d'encadrement qui en découlent, assurent le respect des obligations ministérielles, des lois et règlements en vigueur et prend en considération les meilleures pratiques reconnues mondialement en matière de sécurité de l'information.

2. Domaine d'application

2.1. Actifs informationnels

La politique sur la sécurité de l'information s'applique à tout actif informationnel détenu et utilisé par le CISSS dans le cadre de sa mission, quel que soit son support (papier ou numérique) et son lieu de conservation (locaux internes, tiers, infonuagique, etc.).

2.2. Intervenants concernés

La politique s'applique à toutes les personnes physiques ou morales qui font usage des actifs informationnels du CISSS des Laurentides.

Les personnes visées peuvent être des médecins, des résidents en médecine, des pharmaciens, des dentistes, des membres du personnel, des membres du conseil d'administration, des personnes travaillant sur une base contractuelle, des entreprises liées par contrat, des stagiaires, des sages-femmes, des bénévoles ou des fournisseurs.

Elle s'applique également aux usagers, à leurs familles et aux visiteurs lorsque ceux-ci font usage des actifs informationnels du CISSS (borne, cellulaire, iPad, etc.).

3. Objectif général et objectifs spécifiques

La présente politique a pour objectif d'encadrer les orientations et activités du CISSS des Laurentides en matière de sécurité de l'information. Plus précisément, elle vise à :

- Assurer la disponibilité de l'information en temps voulu et de la manière requise par une personne autorisée ;
- Assurer l'intégrité de l'information au moyen d'un support qui lui procure la stabilité et la pérennité de celle-ci ;
- Assurer l'intégrité de l'information en encadrant la modification et la destruction de celle-ci ;
- Assurer la confidentialité de l'information aux seules personnes autorisées à en prendre connaissance.

4. Fondements

Les lois, règlements et autres documents précisant les obligations légales ou administratives qui encadrent la présente politique sont présentés à l'annexe 2.

5. Énoncé(s)

5.1. PRINCIPES DIRECTEURS

Les six (6) principes présentés pour assurer la mise en œuvre de la gestion de la sécurité de l'information au CISSS des Laurentides servent de référence pour guider les décisions et orienter les comportements.

5.1.1. Gouvernance

Le président-directeur général du CISSS des Laurentides s'assure de déployer un processus de gestion intégrée de la sécurité de l'information et valorise l'amélioration continue des pratiques en la matière.

La politique constitue le document maître de la sécurité de l'information et en complément, les rôles et responsabilités sont décrits dans le *Cadre de gestion de la sécurité de l'information du CISSS des Laurentides*.

5.1.2. Responsabilité et imputabilité

Les processus de gestion en sécurité de l'information sont soutenus par des pratiques éthiques visant à réguler les conduites et à favoriser la responsabilisation individuelle de chaque personne visée. Ainsi, la sécurité de l'information au sein de l'organisme représente une responsabilité collective.

L'imputabilité organisationnelle s'actualise par les activités de reddition de comptes. La transparence est la principale valeur qui guide le responsable de la sécurité de l'information (RSI) dans ce type d'activités puisqu'elle permet la priorisation juste des actions.

5.1.3. Amélioration continue

Les orientations de sécurité de l'information émises et documentées par le CISSS doivent correspondre à des façons de faire reconnues à l'échelle provinciale, nationale ou internationale (lois, normes, meilleures pratiques, etc.). Afin de s'assurer que les pratiques respectent les orientations organisationnelles, des mécanismes d'audit sont mis en place.

5.1.4. Équipement et propriété des données

Les technologies de l'information déployées et/ou utilisées dans le cadre des activités de l'organisation sont autorisées par la Direction des ressources informationnelles (DRI) et le responsable de la sécurité de l'information.

De plus, toute information installée dans les actifs informationnels du CISSS est sous la gouverne du MSSS et du PDG qui doivent en assurer la sécurité.

5.1.5. Droit de regard

Le CISSS des Laurentides exerce un droit de regard sur tout usage des actifs informationnels de l'établissement, en conformité avec la législation et la règlementation en vigueur, ainsi qu'avec les normes entourant le droit au respect de la vie privée.

Par les pouvoirs qui lui sont octroyés, le responsable de la sécurité de l'information (RSI) ou la personne qu'il délègue (conseiller en gouvernance, officier de sécurité, pilote de système, etc.) peut examiner l'utilisation des actifs informationnels. Ce dernier peut intervenir lorsqu'il détecte une situation réelle ou potentielle de non-conformité à ses politiques et directives.

5.1.6. Formation et sensibilisation

La sensibilisation et la formation sont indispensables pour le développement d'un personnel compétent et engagé en matière de sécurité de l'information.

Chaque utilisateur a l'obligation de s'engager à lire et respecter les exigences en matière de sécurité de l'information.

De plus, le programme de formation permet d'améliorer la posture de sécurité de l'établissement et ainsi promulguer une offre de services sécuritaire en matière de sécurité de l'information à la population des Laurentides.

5.2. ORIENTATIONS

La gestion de la sécurité demande la mise en place d'un ensemble de mesures coordonnées et adaptées à la mission du CISSS des Laurentides. Ces mesures supportent les besoins d'affaires et sont encadrées par des exigences de sécurité et des pratiques reconnues.

Dans cet esprit, la politique sur la sécurité de l'information s'articule autour de trois axes fondamentaux de gestion : la gestion des accès, des risques et des incidents.

5.2.1. Gestion des identités et des accès

La gestion des accès et des identités doit être encadrée et contrôlée pour faire en sorte que l'accès, la divulgation et l'utilisation de l'information soient disponibles aux personnes autorisées, et ce, en fonction des tâches confiées.

5.2.2. Gestion des risques

La gestion des risques de la sécurité de l'information s'inscrit dans le processus global de gestion intégrée des risques au sein du CISSS des Laurentides et représente une responsabilité organisationnelle.

Elle requiert la mise en place d'un système qui permet l'identification, l'analyse et le traitement des risques de sécurité à tous les niveaux hiérarchiques de l'organisation.

Le CISSS des Laurentides s'engage à :

- Évaluer régulièrement les risques organisationnels;
- Mettre en place des mesures proactives de sécurité et des méthodes de détection d'usage abusif ou inapproprié de l'information;
- Définir des actions d'éradication des menaces ou de recouvrement des activités compromises.

5.2.3. Gestion des incidents

La gestion des incidents permet la prise en charge d'incidents susceptibles de compromettre la sécurité de l'information et d'affecter la prestation de services.

À cet égard, le CISSS met en place les mesures nécessaires en vue de :

- Minimiser l'occurrence des incidents en matière de sécurité de l'information ;
- Gérer adéquatement ces incidents pour en minimiser les conséquences et rétablir les activités ou les opérations ;
- S'assurer d'une communication efficace dans les situations pouvant affecter les actifs informationnels ;
- Informer le responsable de la sécurité de l'information de tout manquement à la sécurité de l'information ;
- Déclarer les incidents de sécurité de l'information au MSSS conformément à la *Directive sur la sécurité de l'information gouvernementale*.

6. Rôles et responsabilités

Le cadre de gestion de la sécurité de l'information du CISSS définit la structure de gouvernance de la sécurité de l'information de même que les rôles et responsabilités des différents acteurs devant œuvrer en partenariat afin d'assurer la performance de la sécurité de l'information pour notre établissement.

Pour l'inventaire complet, vous référer au *Cadre de gestion de la sécurité de l'information du CISSS des Laurentides*.

6.1. Conseil d'administration

Le conseil d'administration adopte la politique sur la sécurité de l'information ainsi que toute modification à celle-ci.

6.2. Dirigeant de l'organisme (PDG)

Le président-directeur général est l'ultime responsable de la sécurité de l'information relevant de son autorité et il prend les moyens nécessaires à la mise en œuvre de la politique et à la gestion de la sécurité de l'information.

Il est responsable devant le ministre de la Santé et des Services sociaux et conserve ses responsabilités dans toute forme d'impartition.

Il autorise, de façon exceptionnelle, une dérogation aux dispositions de la présente politique, d'une directive ou d'une procédure ayant une incidence directe ou indirecte sur la sécurité de l'information et qui serait incompatible avec une activité reliée à la mission du CISSS.

Il assure les actions requises lorsqu'un membre de son personnel ne respecte pas les consignes émises et que cette situation met en péril la protection des renseignements personnels de la population des Laurentides.

6.3. Responsable de la sécurité de l'information (RSI)

Sous l'autorité immédiate du président-directeur général, le responsable de la sécurité de l'information gère et coordonne la sécurité de l'information.

Il planifie les activités nécessaires à la mise en place de la sécurité de l'information, entre autres, l'élaboration et l'application de la présente politique et du cadre de gestion en sécurité de l'information.

Il préside, pour le PDG, le comité de sécurité de l'information et lui soumet pour consultation les événements ayant mis ou qui auraient pu mettre en péril la sécurité de l'information de l'organisme ainsi que toute proposition d'action ou état d'avancement des projets liés à la sécurité de l'information.

6.4. Conseiller en gouvernance de la sécurité de l'information (CGSI)

Le conseiller en gouvernance de la sécurité de l'information (CGSI) apporte son soutien au RSI notamment en ce qui concerne l'encadrement de la sécurité de l'information, le choix des moyens et à la planification des actions en sécurité. En l'absence du RSI, c'est le conseiller en gouvernance de la sécurité qui fera office de RSI.

6.5. Officier de sécurité de l'information (OSI)

L'officier de sécurité de l'information (OSI) est un professionnel des technologies de l'information et à ce titre, il apporte conseil et assistance aux RSI et CGSI.

6.6. Responsables de secteurs connexes

La sécurité de l'information est une responsabilité collective et les responsables de domaines connexes contribuent avec le RSI à sa mise en œuvre en veillant au respect des exigences de sécurité relatives à leur domaine.

Les responsables des secteurs connexes sont identifiés dans le *Cadre de gestion de la sécurité de* l'information et la liste des responsables CISSS est accessible sur l'intranet.

6.7. Détenteurs de l'information

Un détenteur d'actif est un membre du personnel-cadre détenant la plus haute autorité au sein d'une unité ou d'un service clinique ou administratif. Son rôle consiste notamment, d'un point de

vue décisionnel, fonctionnel ou opérationnel, à veiller à l'accessibilité, à l'utilisation adéquate, à la gestion efficiente et à la sécurité des actifs informationnels sous sa responsabilité. Il collabore étroitement avec le RSI, le CGSI et l'OSI notamment pour la catégorisation des actifs informationnels, la détermination des exigences de sécurité, la gestion des incidents et la reddition de comptes en matière de sécurité.

6.8. Comité de sécurité de l'information (CSI)

Le comité de sécurité de l'information relève du président-directeur général et constitue un mécanisme de coordination et de concertation qui, par sa vision globale, est en mesure de proposer des orientations et de faire des recommandations au PDG et au conseil d'administration.

Le mandat ainsi que la composition du comité se retrouvent sur l'intranet.

6.9. Directeurs et gestionnaires

Le gestionnaire (cadre supérieur ou intermédiaire) est responsable de l'application et du respect de la présente politique au sein de son unité administrative, de même que de l'application des directives touchant la sécurité de l'information et des bonnes pratiques en cette matière.

Il sensibilise régulièrement les membres de son personnel à la protection de l'information, aux conséquences d'une atteinte à la sécurité de l'information ainsi qu'à leurs responsabilités en la matière.

Il collabore étroitement avec le RSI, le CGSI et l'OSI et il leur fournit le soutien nécessaire à l'exercice de leurs responsabilités.

6.10. Utilisateurs des actifs

Toute personne autorisée à avoir accès aux actifs informationnels assume des responsabilités notamment en matière de protection de l'information et répond de ses actions auprès du PDG.

Chaque utilisateur se doit de respecter la présente politique ainsi que les directives et procédures en vigueur en matière de sécurité de l'information. À cet effet, il :

- Prend connaissance et adhère à la politique sur la sécurité de l'information ;
- Se conforme aux consignes et directives établies et dans le respect des dispositions de la présente politique ;
- Utilise les actifs informationnels en se limitant aux fins pour lesquelles ils sont destinés et à l'intérieur des accès qui lui sont autorisés ;
- Signale à son gestionnaire, toute violation des mesures de sécurité dont il pourrait être témoin ou de toutes anomalies décelées pouvant nuire à la protection des actifs ;
- Collabore à toute intervention visant à indiquer ou à atténuer une menace à la sécurité de l'information ou à un incident de sécurité de l'information.

7. Modalités d'application de la politique

Le RSI, assisté par le service des communications, des directeurs et des gestionnaires est responsable de la diffusion de la politique.

8. Mesures applicables en cas de non-observance

8.1.1. Mesure d'exception

Le détenteur de l'information qui a une raison valable de ne pas se conformer à une exigence particulière ou de ne pas recourir à une mesure de sécurité déterminée peut demander une mesure d'exception au RSI après avoir pris soin d'évaluer les risques associés à cette mesure d'exception.

Toute demande d'exception à une consigne de sécurité est prise en charge par l'équipe de sécurité de l'information du CISSS.

En cas d'urgence, la mesure d'exception peut être autorisée par le gestionnaire responsable du secteur visé. Ce gestionnaire en fait rapport au RSI.

8.2. Sanctions

En cas de non-respect de la présente politique ou des documents en découlant, l'utilisateur engage sa responsabilité personnelle et peut être soumis à des sanctions.

Les mesures applicables peuvent être de différents ordres et sont déterminées en fonction de la nature, la gravité et les conséquences de l'acte commis.

- Pour les employés, ces sanctions peuvent aller d'un simple rappel jusqu'au congédiement ;
- Pour les médecins, partenaires, les mandataires et les fournisseurs, ces derniers sont passibles de mesures administratives, par exemple, la résiliation du contrat ou l'expulsion de la personne qui travaille pour son compte.

Enfin, des poursuites criminelles ou pénales pourraient être intentées contre toute personne qui enfreindrait l'une de ces règles.

9. Mécanisme de suivi et de révision

Le suivi de la politique est assuré de manière continue dans les différentes actions posées quotidiennement par les utilisateurs du CISSS des Laurentides. De plus, un bilan annuel de la sécurité est mené sous la gouverne du MSSS.

Cette politique entre en vigueur à la date de son adoption par le Conseil d'administration et sera révisée au besoin, mais au minimum tous les 3 ans de sa date d'entrée en vigueur.

10. Demande de renseignements

Pour avoir accès à la politique et autres documents concernant la sécurité de l'information, veuillez-vous référer au site intranet du CISSS.

Pour une interprétation du texte ou pour une demande de renseignements concernant la présente politique, veuillez communiquer avec :

Service de la gestion stratégique de l'information (GSI)
Direction de la qualité, de l'évaluation, de la performance et de l'éthique
Centre intégré de santé et de services sociaux des Laurentides
500, boulevard des Laurentides, local 011
Saint-Jérôme, Québec J7Z 4M2
Courriel : equipe_gsi@ssss.gouv.qc.ca

Annexe 1 : Définitions

Les termes employés dans le présent cadre de gestion ainsi que dans les documents d'encadrement font l'objet d'une définition dans le glossaire de la gestion de l'information - LI 2017 DPACQ 012.

Annexe 2 : Cadre légal et administratif

La présente politique s'inscrit principalement dans un contexte régi par :

- 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 ;
- Loi concernant le cadre juridique des technologies et l'information, L.R.Q., c. C-1.1 ;
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, L.R.Q., c. A-2.1 ;
- Loi sur la protection des renseignements personnels dans le secteur privé ;
- Loi sur la protection des renseignements personnels et les documents électroniques ;
- Loi sur le droit d'auteur, L.R., 1985, c. C-42 ;
- Loi sur les services de santé et les services sociaux, L.R.Q., c. S-4.2 ;
- Loi modifiant l'organisation et la gouvernance du réseau de la santé et des services sociaux notamment par l'abolition des agences régionales ;
- Loi sur les services de santé et les services sociaux pour les autochtones cris, L.R.Q., c. S-5 ;
- Loi sur les services préhospitaliers d'urgence, L.R.Q, c. S-6.2;
- Loi sur la Régie de l'assurance maladie du Québec, L.R.Q., c.R-5;
- Loi sur l'assurance maladie, L.R.Q., c. A-29, section VII ;
- Loi médicale, L.R.Q., c. M-9;
- Loi sur la pharmacie, L.R.Q., c. P-10;
- Loi sur la santé publique, L.R.Q., c. S-2.2;
- Loi sur la protection de la jeunesse, L.R.Q., c. P-34.1;
- Loi sur le curateur public, L.R.Q., c. C-81;
- Loi sur la santé et la sécurité au travail, L.R.Q., c. S-2.1;
- Loi sur les accidents de travail et les maladies professionnelles, L.R.Q., c. A-3.001;
- Loi sur la recherche des causes et des circonstances de décès, L.R.Q., c. R-0.2;
- Code des professions, L.R.Q., c. C-26, articles 60.4 à 60.6 et 87;
- Codes de déontologie des différents ordres professionnels œuvrant dans le domaine de la santé et des services sociaux;
- Règlement sur la diffusion de l'information et sur la protection des renseignements personnels, c. A-2.1, r. 02;
- Charte des droits et libertés de la personne, L.R.Q., c. C-12;
- Code civil du Québec, L.Q., 1991, c. 64;
- Loi sur les archives, L.R.Q., c. A-21.1;
- Loi sur l'administration publique, L.R.Q., c. A-6.01;
- Loi sur la fonction publique, L.R.Q., c. F-3.1.1;
- Loi canadienne sur les droits de la personne, L.R., 1985, c. H-6;
- Code criminel, L.R., 1985, c. C-46;
- Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics;
- Directive sur la sécurité de l'information gouvernementale, décret 7-2014;
- Loi sur le système de justice pénale pour les adolescents, L.C. 2002, ch. 1.