Centre intégré
de santé
et de services sociaux
de Lanaudière
Québec

Direction des ressources informationnelles
Lanaudière – Laurentides – Laval

Cadre de gestion
de la sécurité de l'information
du CISSS de Lanaudière

Mai 2016

TABLE DES MATIÈRES

1 PRÉAMBULE

Suite au Cadre gouvernemental de gestion de la sécurité de l'information adopté par le Secrétariat du Conseil du trésor (SCT), le ministère de la Santé et des Services sociaux (MSSS) a établi une politique et un cadre de gestion de la sécurité de l'information s'appliquant à tous les établissements du réseau de la santé.

Le présent cadre de gestion de la sécurité de l'information définit les rôles et responsabilités en matière de sécurité de l'information au CISSS de Lanaudière. Il découle de la politique de sécurité de l'information du CISSS et est subordonné à la politique provinciale de sécurité de l'information du MSSS et au cadre de gestion de la sécurité de l'information (CGSI) du MSSS.

2 CHAMP D'APPLICATION

Le présent cadre de gestion est applicable au CISSS de Lanaudière.

Le champ d'application est celui défini dans la politique de sécurité de l'information du CISSS de Lanaudière.

3 DÉFINITIONS[1]

Pour l'application du présent cadre de gestion, les termes et expressions suivants signifient:

1° **Actif informationnel** : actif informationnel au sens de la LPCRS[2], soit, une banque d'informations, un système d'information, un réseau de télécommunication, une infrastructure technologique ou un ensemble de ces éléments ainsi qu'une composante informatique d'un équipement médical spécialisé ou ultraspécialisé.

Est également considéré comme un actif informationnel, tout support papier contenant de l'information.

2° **Détenteur de l'information** : un employé désigné par son organisme public, appartenant à la classe d'emploi de niveau-cadre ou à une classe d'emploi de niveau supérieur, et dont le rôle est, notamment, de s'assurer de la sécurité de l'information et des ressources qui la sous-tendent, relevant de la responsabilité de son unité administrative. Le terme « détenteur de processus d'affaires » est utilisé lorsque ce rôle se limite à un processus d'affaires déterminé.

3° **Utilisateur** : toute personne de l'organisme de quelque catégorie d'emploi, de statut d'employé ainsi que toute personne morale ou physique qui, par engagement contractuel ou autrement, utilise un actif informationnel sous la responsabilité de l'organisme ou y a accès.

4° **Réseau** : ensemble des organismes qui relèvent du dirigeant réseau de l'information (DRI) de la santé et des services sociaux en vertu de l'article 2, paragraphe 5 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LGGRI).

5° **Système d'information** : système constitué des ressources humaines (le personnel), des ressources matérielles (l'équipement) et des procédures permettant d'acquérir, de stocker, de traiter et de diffuser les éléments d'information pertinents pour le fonctionnement d'une entreprise ou d'un organisme.

[1] Extraites du CGSI MSSS
[2] Loi concernant le partage de certains renseignements de santé

4 CADRE LÉGAL ET ADMINISTRATIF

Le cadre légal et administratif applicable est celui défini dans la politique de sécurité de l'information du CISSS de Lanaudière.

5 OBJECTIFS

Le présent cadre de gestion de la sécurité de l'information complète les dispositions de la politique de sécurité de l'information du CISSS et vise à renforcer la gouvernance de la sécurité de l'information au CISSS, par la mise en place d'une structure matricielle de la sécurité de l'information et par la définition de rôles et responsabilités en la matière.

Les rôles et responsabilités définis concernent l'approbation, la mise en place, la coordination, le développement, le suivi et l'évaluation de la sécurité de l'information au CISSS, en tenant compte des exigences du cadre légal et administratif applicable au Réseau de même que des principes généraux de la politique provinciale de sécurité de l'information du MSSS et de la politique de sécurité de l'information du CISSS.

6 STRUCTURE MATRICIELLE DE LA SÉCURITÉ DE L'INFORMATION DU CISSS

Le cadre de gestion de la sécurité de l'information met en oeuvre la structure matricielle requise pour assurer une gouvernance forte et intégrée, pour favoriser la concertation entre les composantes du CISSS et d'autres organismes, pour profiter de la complémentarité de leurs ressources et pour optimiser l'efficacité de leurs actions.

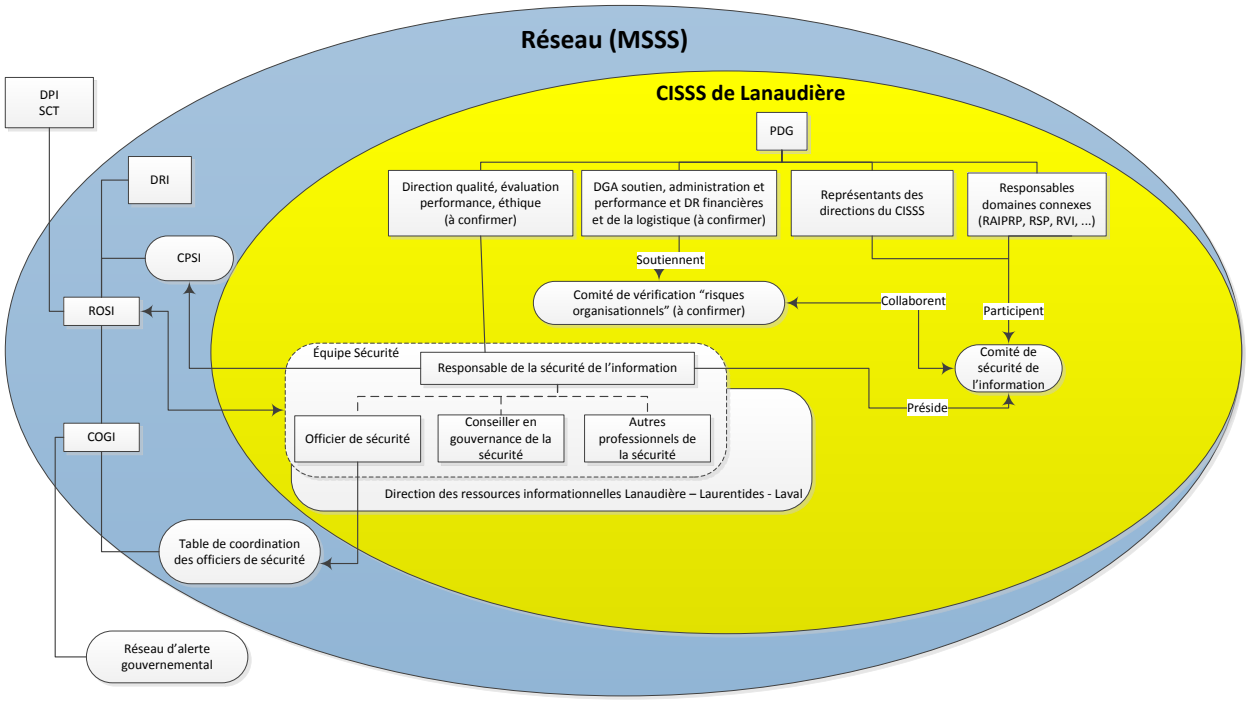

Figure 1 Structure matricielle[3] de la sécurité de l'information au CISSS de Lanaudière. Notez que l'équipe sécurité représente les rôles devant être assumés et non les individus.

7 RÔLES ET RESPONSABILITÉS

Cette section est structurée en présentant d'abord les rôles et responsabilités tels qu'ils sont énoncés dans le cadre de gestion de l'information du MSSS (CGSI), puis en déclinant, lorsque nécessaire, les éléments spécifiques au contexte suprarégional (LLL) suivi de ceux spécifiques au contexte du CISSS.

7.1 Le conseil d'administration de l'organisme

Le conseil d'administration de l'organisme :

1˚ adopte la politique et le plan d'action établis par l'organisme en matière de sécurité de l'information, lesquels sont conformes à la Politique provinciale de sécurité de l'information et au cadre de gestion de la sécurité de l'information, et suit leur application dans l'établissement;

2˚ reçoit et entérine annuellement ou au besoin le Bilan de sécurité de l'information de l'organisme.

7.2 Le dirigeant de l'organisme

En tant que premier responsable de la sécurité de l'information de son organisme, le dirigeant d'un organisme public :

[3] COGI : coordonnateur organisationnel de la gestion des incidents
CPSI : comité provincial de sécurité de l'information
DPI SCT : dirigeant principal de l'information, Secrétariat du Conseil du trésor
DRI : dirigeant réseau de l'information
RAIPRP: responsable de l'accès à l'information et de la protection des renseignements personnels
ROSI : responsable organisationnel de la sécurité de l'information
RSP: responsable de la sécurité physique
RVI: responsable de la vérification interne

1° s'assure du respect des lois et des règles de sécurité de l'information s'appliquant au Réseau, notamment celles émises par le Secrétariat du Conseil du trésor (SCT);

2° approuve le cadre de gestion de la sécurité de l'information adapté à son organisme;

3° s'assure de la mise en oeuvre de la politique de sécurité de l'information adoptée par le conseil d'administration et des rôles et responsabilités du cadre de gestion de la sécurité de son organisme;

4° nomme un employé de la classe d'emploi cadre à titre de Responsable de la sécurité de l'information (RSI) de son organisme et s'assure de lui octroyer les pouvoirs et ressources nécessaires à la réalisation de ses tâches et responsabilités. Le formulaire de nomination du RSI doit être retourné annuellement au 1er avril ou, au besoin, au ROSI lors d'un changement du RSI;

5° établit avec son RSI une relation de forte collaboration lui permettant d'être au fait de toute situation à risque et de tout incident majeur de sécurité de l'information;

6° informe et mobilise ses gestionnaires et l'ensemble de son personnel au sujet de l'application des bonnes pratiques en sécurité de l'information;

7° s'assure de la gestion adéquate des risques de sécurité de l'information en lien avec son contexte organisationnel;

8° s'assure de la nomination des détenteurs de la sécurité de l'information pour son organisme afin d'assurer la sécurité de l'information et des ressources qui la sous-tendent;

9° s'assure de la mise en place d'un comité chargé de la sécurité de l'information au sein de son organisme et mandate le RSI pour présider ce comité.

7.3 Le responsable de la sécurité de l'information (RSI) de l'organisme

Le RSI est un cadre de la fonction publique du Québec, nommé par le dirigeant de son organisme. Cette personne a les pouvoirs et les compétences nécessaires à la gestion de la sécurité de l'information de son organisme. À ce titre, il :

1° planifie les activités nécessaires à la mise en place de la sécurité de l'information au sein de son organisme;

2° s'assure de l'encadrement de la sécurité de l'information au sein de son organisme, veille à l'application de la politique et du cadre de gestion de la sécurité de l'information de son organisme et s'assure du respect, par son organisme, des règles particulières publiées par le DRI[4] en matière de sécurité de l'information;

3° agit à titre de porte-parole du ROSI auprès de son organisme en informant les différents intervenants en sécurité de l'information, des orientations et des priorités d'intervention provinciale et s'assure de leur mise en oeuvre;

4° représente son organisme au Comité provincial de la sécurité de l'information du Réseau et s'assure de la participation de son organisme aux processus provinciaux de gestion de la sécurité de l'information;

[4] Dirigeant réseau de l'information (sigle MSSS)

5˚ dirige la coordination et la cohérence des activités de sécurité de l'information menées au sein de son organisme, notamment celles de son officier de sécurité de l'information et de son conseiller en gouvernance de la sécurité, le cas échéant;

6˚ préside, pour le compte du dirigeant de l'organisme, le comité de sécurité de l'information au sein de son organisme et lui soumet, pour consultation, les orientations, les politiques, les directives, les cadres de gestion, les plans d'action, les bilans et les rapports sur 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 destinés au dirigeant de l'organisme;

7˚ s'assure de la mise en place du registre d'autorité de la sécurité de l'information, dans lequel sont notamment consignés les noms des détenteurs de l'information et les systèmes d'information qui leur sont assignés;

8˚ s'assure de la mise en oeuvre d'un système de gestion intégré des risques de sécurité de l'information, qui lui permet de maîtriser les risques de sécurité relatifs à son organisme;

9˚ s'assure de la mise en oeuvre d'un processus de gestion des incidents de sécurité de l'information dans son organisme;

10˚ veille à l'identification et à la prise en charge des exigences de sécurité de l'information lors de la réalisation de projets de développement ou de l'acquisition de systèmes d'information;

11˚ s'assure de l'intégration aux ententes de services et aux contrats, des dispositions garantissant le respect des exigences de sécurité de l'information en prenant appui sur le cadre gouvernemental d'élaboration de clauses contractuelles en matière de sécurité de l'information et de protection des renseignements personnels;

12˚ veille à la mise en oeuvre de toute recommandation jugée pertinente découlant d'une vérification ou d'un audit de sécurité;

13˚ s'assure de l'élaboration et de la mise en oeuvre d'un programme formel de formation et de sensibilisation en matière de sécurité de l'information;

14˚ s'assure de la production d'un bilan annuel ou, au besoin, d'un plan d'action triennal de la sécurité de l'information de son organisme, les valide et les transmet au ROSI du Réseau et à son dirigeant d'organisme;

15˚ rend compte des réalisations de son organisme en matière de sécurité de l'information au ROSI du Réseau et à son dirigeant d'organisme;

16˚ évalue constamment toute information reçue en lien avec la sécurité de l'information.

Le RSI a une écoute particulière du dirigeant de l'organisme qui l'a nommé et réfère à celui-ci pour toute situation exceptionnelle qui pourrait mettre en péril la sécurité de l'information de l'organisme.

Contexte suprarégional :

17˚ travaille de concert avec les instances de niveau suprarégional;

18˚ s'assure du respect par son organisme, des règles particulières publiées par la Direction des ressources informationnelles LLL en matière de sécurité de l'information.

Contexte CISSS :

19˚ s'assure de l'arrimage des actions en sécurité de l'information avec la Direction qualité évaluation performance éthique.

7.4 Le conseiller en gouvernance de la sécurité de l'organisme

Le conseiller en gouvernance de la sécurité de l'information apporte son soutien au RSI de son organisme, notamment en ce qui concerne l'encadrement de la sécurité de l'information, le choix des moyens pour satisfaire aux exigences des règles particulières adoptées par le DRI[5] et à la planification des actions en sécurité. À cet égard, il :

1˚ accompagne le RSI dans la définition des orientations stratégiques, des directives et des plans d'action en matière de sécurité de l'information;

2˚ participe à la rédaction des documents d'encadrement de la sécurité de l'information de son organisme, notamment la politique et le cadre de gestion de sécurité de l'information;

3˚ accompagne le RSI dans la mise en oeuvre des orientations internes découlant des directives ministérielles et de celles du DRI[6], des politiques internes et des pratiques généralement admises à cet égard;

4˚ participe à la définition et accompagne le RSI dans la mise en oeuvre de processus formels de gestion de la sécurité de l'information;

5˚ accompagne les directions partenaires en matière de sécurité de l'information et participe à l'intégration de dispositions garantissant le respect des exigences de sécurité de l'information dans les ententes de service et les contrats;

6˚ assiste les détenteurs de l'information dans la catégorisation de l'information relevant de leur responsabilité, dans l'identification et l'évaluation des situations de risques ainsi que dans la définition de plans d'action visant à réduire les risques de sécurité de l'information à un niveau acceptable pour l'organisme et pour le MSSS;

7˚ identifie et prend en charge les exigences de sécurité de l'information lors de la réalisation de projets de développement ou de l'acquisition de systèmes d'information;

8˚ élabore et met en oeuvre le programme de formation et de sensibilisation en matière de sécurité de l'information;

9˚ tient à jour le registre d'autorité de la sécurité de l'information;

10˚ assure la coordination et la réalisation de projets de sécurité de l'information;

11˚ produit les bilans et les plans d'action de sécurité de l'information de son organisme.

Contexte suprarégional

12˚ travaille de concert avec les instances de niveau suprarégional.

7.5 L'officier de sécurité de l'information

L'officier de sécurité de l'information est un professionnel de la sécurité de l'information ayant les compétences nécessaires à la réalisation des tâches et responsabilités suivantes. Il :

1˚ contribue à la mise en place des activités opérationnelles de sécurité de l'information, plus précisément, la planification, le déploiement, l'exécution, la surveillance, les enquêtes et

[5] Dirigeant réseau de l'information (sigle MSSS)
[6] Dirigeant réseau de l'information (sigle MSSS)

l'amélioration des processus de sécurité nécessaires à la gestion opérationnelle de la sécurité dans son organisme, la gestion des risques et la gestion des incidents en respectant les exigences de sécurité définies dans les règles particulières et conformément aux pratiques recommandées de l'industrie;

2˚ participe activement au réseau d'alerte du Réseau pour la gestion des incidents de sécurité de l'information;

3˚ contribue aux analyses de risques de sécurité de l'information, identifie les menaces et les situations de vulnérabilité et met en oeuvre les solutions appropriées;

4˚ soutient le RSI et le conseiller en gouvernance de la sécurité dans les activités de développement et d'acquisition, pour le volet technique de la sécurité dans le respect des exigences de sécurité définies dans les règles particulières et conformément aux pratiques recommandées;

5˚ participe aux comités de gestion des changements, s'il y a lieu, et possède un droit de réserve face à des changements qu'il juge trop risqués sur le plan de la sécurité de l'information;

6˚ s'assure de la production des rapports des processus de sécurité de l'information (incidents, vulnérabilités, etc.) et les transmet à son RSI, avec son appréciation et des justifications, au besoin.

Contexte suprarégional :

7˚ travaille de concert avec les instances de niveau suprarégional;

8˚ collabore étroitement avec la direction des ressources informationnelles LLL pour tout projet, action ou incident de sécurité de l'information à portée suprarégionale.

7.6 Le Comité de sécurité de l'information de l'organisme

Le Comité de sécurité de l'information est l'instance de concertation en matière de sécurité de l'information de l'organisme. Plus particulièrement, il :

1˚ examine et formule des recommandations concernant les orientations, les politiques, les directives, les cadres de gestion, les plans d'action et les bilans de l'organisme, ainsi que toute proposition d'action ou état d'avancement de projets en sécurité de l'information;

2˚ s'assure de la prise en charge des risques, des situations vulnérables ou des incidents identifiés;

3˚ analyse et formule des recommandations concernant les événements ayant mis ou qui auraient pu mettre en péril la sécurité de l'information de l'organisme.

Contexte CISSS :

4˚ s'arrime avec le Comité de gestion des risques et le Comité de vérification pour traiter les dossiers communs le plus efficacement possible;

5˚ collabore étroitement avec le Comité de gestion des risques pour prévenir, documenter, et résoudre les incidents reliés à la sécurité de l'information et en assurer le suivi;

6° s'assure que l'expérience client ne soit pas atténuée à cause des exigences de sécurité de l'information, bien que ces dernières soient requises;

7° s'assure que les besoins d'affaires soient répondus de façon sécuritaire.

Ce comité est présidé par le RSI, à titre de représentant du dirigeant de l'organisme. Il est constitué des détenteurs de l'information ainsi que des unités administratives responsables des ressources informationnelles, de la vérification interne, de l'accès à l'information et de la protection des renseignements personnels, de la gestion documentaire, de la sécurité physique et de l'éthique, ainsi que, sur invitation, toute personne jugée pertinente.

7.7 Le Comité de gestion des risques de l'organisme[7]

Contexte CISSS :

Dans une vision où la sécurité de l'information n'est pas uniquement reliée à la technologie, le Comité de gestion des risques doit être un acteur important. Notamment, il :

1˚ s'arrime avec le Comité de sécurité de l'information pour traiter les dossiers communs le plus efficacement possible;

2˚ collabore étroitement avec le Comité de sécurité de l'information pour prévenir, documenter, et résoudre les incidents reliés à la sécurité de l'information et en assurer le suivi.

7.8 Les responsables de domaines connexes à la sécurité de l'information

Les responsables de domaines connexes à la sécurité veillent au respect des exigences de sécurité relatives à leur domaine. À ce titre, ils :

1˚ communiquent au RSI de l'organisme les problématiques et les préoccupations de sécurité en rapport avec leur domaine;

2˚ contribuent à assurer la cohérence et l'harmonisation des interventions en sécurité de l'information, y compris lors de la mise en oeuvre du processus de gestion des risques et des incidents de sécurité de l'information;

3˚ participent au comité de sécurité de l'information de l'organisme.

Selon les organismes, il peut s'agir notamment, sans s'y limiter, du :

1˚ responsable de la gestion des technologies de l'information;

2˚ responsable de l'architecture d'entreprise, volet sécurité;

3˚ responsable de l'accès à l'information et de la protection des renseignements personnels;

4˚ responsable de la vérification interne;

5˚ responsable de la sécurité physique;

6˚ responsable de la gestion documentaire;

7˚ responsable de la continuité des services;

8˚ responsable de l'éthique;

9˚ responsable de la gestion de la qualité et des risques organisationnels.

[7] Rôle non présent dans le CGSI du MSSS et ajouté dans le contexte CISSS.

7.9 Les détenteurs de l'information

Les détenteurs de l'information sont responsables d'assurer la sécurité d'un actif informationnel ou de plusieurs, qui leur sont confiés par le sous-ministre ou le dirigeant de l'organisme. Notamment, ils :

1˚ s'impliquent dans l'ensemble des activités relatives à la sécurité, notamment la catégorisation, l'évaluation des risques, la détermination du niveau de protection visé, l'élaboration des contrôles non technologiques et, finalement, la prise en charge des risques résiduels;

2˚ s'assurent de connaître et évaluer les risques et vulnérabilités de leurs actifs informationnels, priorisent les actions correctives appropriées et gèrent leur application selon le plan d'action déterminé;

3˚ s'assurent que les mesures de sécurité appropriées sont élaborées, approuvées, mises en place et appliquées systématiquement;

4˚ s'assurent que leur nom et les actifs informationnels dont ils assument la responsabilité sont consignés dans le registre d'autorité;

5˚ déterminent les règles d'accès aux actifs informationnels dont ils assument la responsabilité avec l'appui du RSI de l'organisme.

7.10 Les pilotes de systèmes[8]

Contexte CISSS

Identifiés par le détenteur de l'information, les pilotes de systèmes :

1˚ assurent le fonctionnement sécuritaire d'un actif informationnel dès le début du projet et lors de sa mise en exploitation, le tout, en respectant les règles de sécurité établies;

2˚ contrôlent l'accès logique à tout actif informationnel dont ils ont la responsabilité;

3˚ informent les utilisateurs, lors de l'attribution des accès, de leurs obligations face à l'utilisation des systèmes d'information dont ils sont responsables;

4˚ appliquent les contrôles de qualité et d'intégrité sur les actifs informationnels dont ils ont la responsabilité.

7.11 La direction des ressources informationnelles LLL[9]

Contexte suprarégional

1˚ administre les actifs informationnels qui lui sont confiés, dont des outils de gestion de la sécurité de l'information, en respectant les principes et mesures de sécurité qui découlent des politiques de sécurité de l'information du MSSS et des CISSS ;

2˚ collabore avec les RSI des CISSS, les équipes de sécurité des CISSS à évaluer les risques et améliorer la sécurité des actifs informationnels;

3˚ s'assure de l'application et du respect des éléments de sécurité de l'information dans l'ensemble des projets, activités et ententes qu'elle réalise ou qu'elle met en place;

8 Rôle non présent dans le CGSI du MSSS et ajouté dans le contexte CISSS.
9 Rôle non présent dans le CGSI du MSSS et ajouté dans le contexte suprarégional.

4˚ rapporte aux instances requises tout incident ou événement qui affecte ou qui est susceptible d'affecter la sécurité de l'information; collabore à sa prise en charge et à sa résolution.

7.12 Toute direction qui accueille de nouveaux utilisateurs [10] au CISSS[11]

Contexte CISSS

Régulièrement de nouveaux utilisateurs joignent les différentes équipes du CISSS de Lanaudière. Tous ne passent pas par la même entrée mais tous doivent signer l'engagement à la politique de sécurité de l'information du CISSS.

Selon l'utilisateur impliqué, les principales directions interpellées, et sans s'y limiter, sont :

Médecins et membres du CMDP	Direction des services professionnels
Chercheurs	Direction de la recherche
Employés	Direction des ressources humaines, communications et affaires juridiques
Résidents	Direction de l'enseignement universitaire
Stagiaires	Direction des soins infirmiers Direction des services multidisciplinaires Direction des ressources humaines, communications et affaires juridiques
Bénévoles	Direction des soins infirmiers Direction des services multidisciplinaires

Ainsi, à chaque nouvel accueil, qui passe ou non par les ressources humaines, la personne qui accueille :

1˚ informe tout nouvel utilisateur, dès son accueil, de ses obligations découlant de la politique de sécurité du CISSS ainsi que des mesures et procédures en vigueur en matière de sécurité de l'information;

2˚ procède à un rappel périodique, au moins une fois l'an, de ces obligations;

3˚ reçoit les demandes d'audit concernant de possibles dérogations aux politiques, mesures, procédures et règles de sécurité de l'information et à l'utilisation éthique des actifs informationnels de la part d'utilisateurs du CISSS sous sa direction, collabore avec le RSI pour monter le dossier d'analyse et établit les mécanismes d'escalade, les actions ou sanctions qui doivent être appliquées.

10 Tiré de la politique sur la sécurité de l'information : L'ensemble du personnel et des professionnels du CISSS, tous les médecins, stagiaires, chercheurs qui ont accès aux dossiers et informations détenues par le CISSS aux fins de leurs fonctions ainsi qu'aux intervenants externes, fournisseurs de services ou tiers qui exercent pour le CISSS. De plus, elle s'étend à toute personne physique ou morale qui utilise ou accède pour le compte du CISSS, ou non, à des informations confidentielles, ou non, quel que soit le support sur lequel elles sont conservées.

11 Rôle non présent dans le CGSI du MSSS et ajouté dans le contexte CISSS.

7.13 Les gestionnaires

Les gestionnaires sont responsables de mettre en oeuvre les dispositions de la politique de sécurité de l'information auprès du personnel relevant de leur autorité. À ce titre, ils :

1˚ informent leur personnel des dispositions de la politique de sécurité de l'information et de toute directive, standard et procédure en vigueur en matière de sécurité de l'information ainsi que des modalités liées à leur mise en oeuvre, et les sensibilisent à la nécessité de s'y conformer;

2˚ s'assurent que les actifs informationnels mis à la disposition de son personnel sont utilisés en conformité avec les principes généraux et les exigences de la politique de sécurité de l'information et des règles particulières;

3˚ s'assurent que la sécurité de l'information est prise en compte dans tout contrat ou entente de service attribué par leur unité administrative et voient à ce que tout consultant, partenaire ou fournisseur s'engage à respecter et respecte les règles de sécurité de l'information de l'organisme.

Contexte CISSS

4˚ contactent les relations de travail pour établir les mécanismes d'escalade et de gradation de sanction lorsque de possibles dérogations à la politique de sécurité de l'information, aux règles de sécurité de l'information, ses mesures, ses procédures et à l'utilisation éthique des actifs informationnels sont observés de la part de leur personnel.

5° contactent le gestionnaire concerné pour toutes situations observées auprès d'utilisateurs ne relevant pas de leur autorité mais pouvant comporter une possible dérogation à la politique de sécurité de l'information, aux règles de sécurité de l'information, ses mesures, ses procédures et à l'utilisation éthique des actifs informationnels.

7.14 Les utilisateurs

Les utilisateurs dûment autorisés à accéder aux actifs informationnels du Réseau:

1˚ appliquent et respectent les lois et règlements qui régissent leur domaine d'activités ainsi que toutes les politiques, directives, mesures et procédures et tous les processus en matière de sécurité de l'information auxquels ils sont assujettis soit par leur lien d'emploi, par contrat ou par entente;

2˚ avisent leur supérieur immédiat de toute situation portée à leur connaissance et qui est susceptible de compromettre la sécurité de l'information.

8 DISPOSITIONS FINALES

Le présent cadre de gestion entre en vigueur à la date de son approbation par le président-directeur général du CISSS de Lanaudière. À compter de cette date, le CISSS de Lanaudière doit procéder à son application dans les délais prescrits.

Le cadre de gestion doit être réévalué minimalement aux trois ans, à chaque modification de la politique provinciale de sécurité de l'information, de la politique de sécurité de l'information du CISSS de Lanaudière et à l'occasion de changements organisationnels ou de nouvelles orientations ministérielles.

Approuvé par : Daniel Castonguay, président-directeur général par lettre à Marc Beaudet, responsable de la sécurité de l'information.

En vigueur le : 2016-05-30