Cadre de gestion de la sécurité de l'information du CHU de Québec-Université Laval

CADRE N^{O} :	**271-10**
Date d'adoption par la PDG :	2016-12-14
Date d'entrée en vigueur :	2016-12-14
Date(s) des révisions :	s/o

Direction des ressources informationnelles

Novembre 2016

TABLE DES MATIÈRES

LISTE DES ABRÉVIATIONS ET SIGLES

CGSI	Conseiller en gouvernance de la sécurité de l'information de l'établissement
DOP	Dirigeant d'un organisme public
DPI	Dirigeant principal de l'information
DRI	Dirigeant réseau de l'information
MSSS	Ministère de la Santé et des Services sociaux
OSI	Officier de sécurité de l'information
RASI	Responsable de l'architecture de sécurité de l'information
RCS	Responsable de la continuité des services
RDASI	Responsable du développement ou de l'acquisition des systèmes d'information
RE	Responsable de l'éthique
RGD	Responsable de la gestion documentaire
RGTI	Responsable de la gestion des technologies de l'information
ROSI	Responsable organisationnel de la sécurité de l'information
RSI	Responsable de la sécurité de l'information
RSP	Responsable de la sécurité physique
RVI	Responsable de la vérification interne

1. CONTEXTE

Le présent cadre de gestion de la sécurité de l'information découle de la nécessité de faire évoluer l'encadrement de la sécurité de l'information aux établissements relevant du ministère de la Santé et des Services sociaux (MSSS), ci-après appelé le « Réseau ». En effet, les rôles et les responsabilités en matière de sécurité de l'information décrits dans le *Cadre global de gestion des actifs informationnels – volet sécurité*, adopté en 2002, n'ont pas été mis à jour. De plus, les nouvelles orientations stratégiques du MSSS visent à renforcer les établissements du Réseau dans une mécanique de reddition de comptes. En outre, la *Loi modifiant l'organisation et la gouvernance du réseau de la santé et des services sociaux notamment par l'abolition des agences régionales*, implique de revoir également la gouvernance de la sécurité de l'information.

Ainsi, le présent cadre de gestion remplace la section II du *Cadre global de gestion des actifs informationnels – volet sécurité* et décrit les rôles et responsabilités en matière de sécurité de l'information dans le Réseau. Ce cadre s'inscrit dans une démarche visant à mettre en œuvre une gouvernance forte et intégrée de la sécurité de l'information. Cette démarche s'appuie sur les documents du Secrétariat du Conseil du trésor.

2. OBJECTIF

Le cadre de gestion de la sécurité de l'information complète les dispositions de la *Politique de sécurité de l'information du CHU de Québec-Université Laval* (n^{o} 271-30) et renforce la gouvernance de la sécurité de l'information par la mise en place d'une structure fonctionnelle de sécurité de l'information et par la définition de rôles et de responsabilités en la matière. Les rôles et responsabilités concernent l'approbation, la mise en place, la coordination, le développement, le suivi et l'évaluation de la sécurité de l'information, en tenant compte des exigences du cadre légal et administratif applicable et des principes généraux de la politique de sécurité de l'information. De plus, le cadre de gestion de la sécurité de l'information s'inscrit dans le cadre normatif, tout en s'appuyant sur le cadre légal et le cadre normatif gouvernemental, tel qu'illustré ci-dessous.

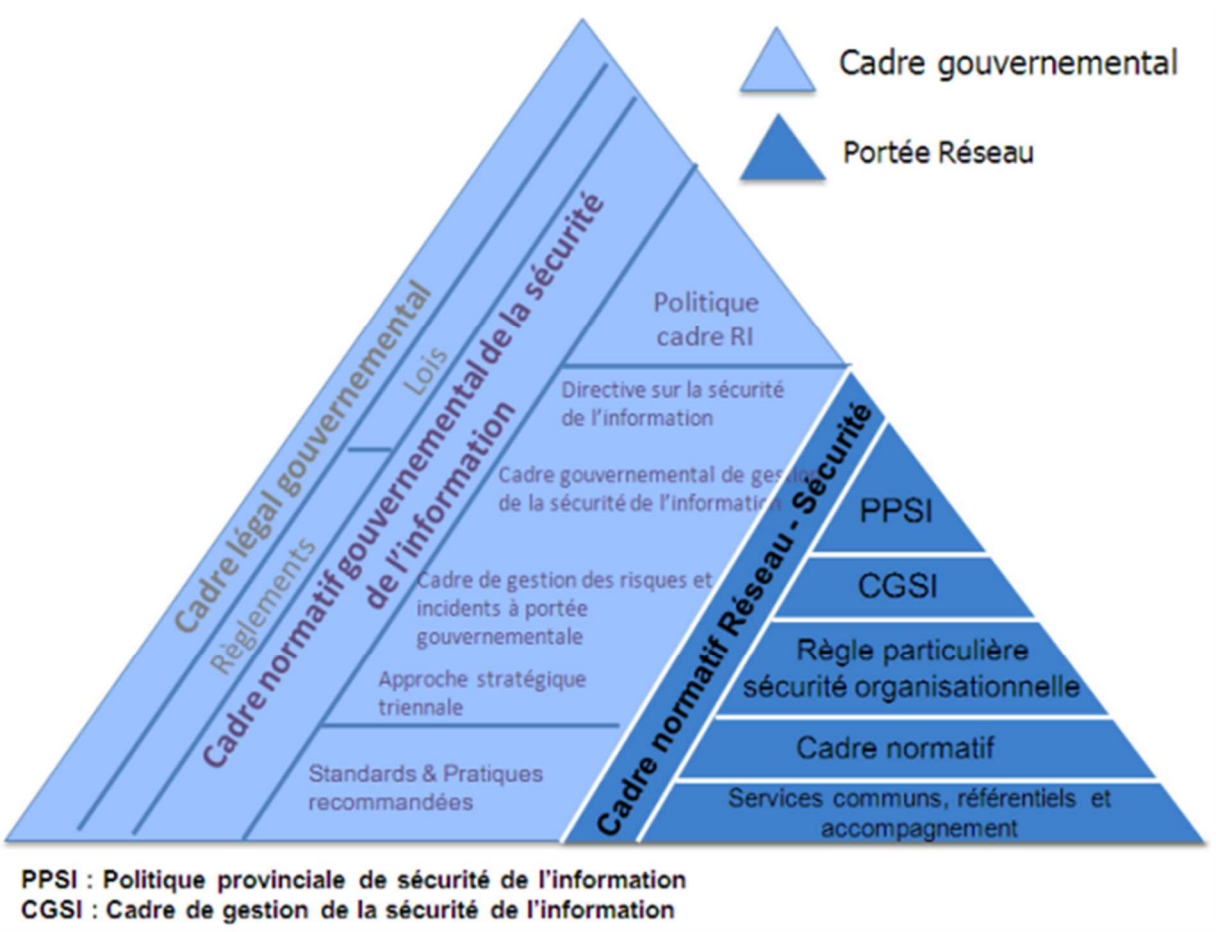


Figure 1: Positionnement du cadre de gestion de la sécurité de l'information du Réseau

3. CHAMP D'APPLICATION

Le présent cadre de gestion s'applique à toute personne physique ou morale qui utilise ou qui peut avoir accès à un ou plusieurs actifs informationnels, peu importe l'endroit où elle se trouve ou la localisation de l'actif. Le champ d'application est celui défini dans le cadre de gestion de sécurité de l'information.

Le cadre de gestion est également assujetti à toute personne physique ou morale dûment autorisée à avoir accès aux actifs informationnels détenus par l'établissement. De plus, l'information visée par le cadre de gestion est celle que l'établissement détient dans l'exercice de sa mission, que sa conservation soit assurée par lui-même ou par un tiers.

4. DÉFINITIONS ET RÉFÉRENCES

Les définitions et les principales références consultées sont présentées dans l'annexe 1 de la *Politique de sécurité de l'information du CHU de Québec-Université Laval.*

5. STRUCTURE FONCTIONNELLE DE LA SÉCURITÉ DE L'INFORMATION DE L'ÉTABLISSEMENT

Le cadre de gestion de la sécurité de l'information met en œuvre la structure fonctionnelle requise pour assurer une gouvernance forte et intégrée, pour favoriser la concertation, pour profiter de la complémentarité des ressources et pour optimiser l'efficacité de leurs actions. Le schéma ci-dessous illustre la structure fonctionnelle de la sécurité de l'information.

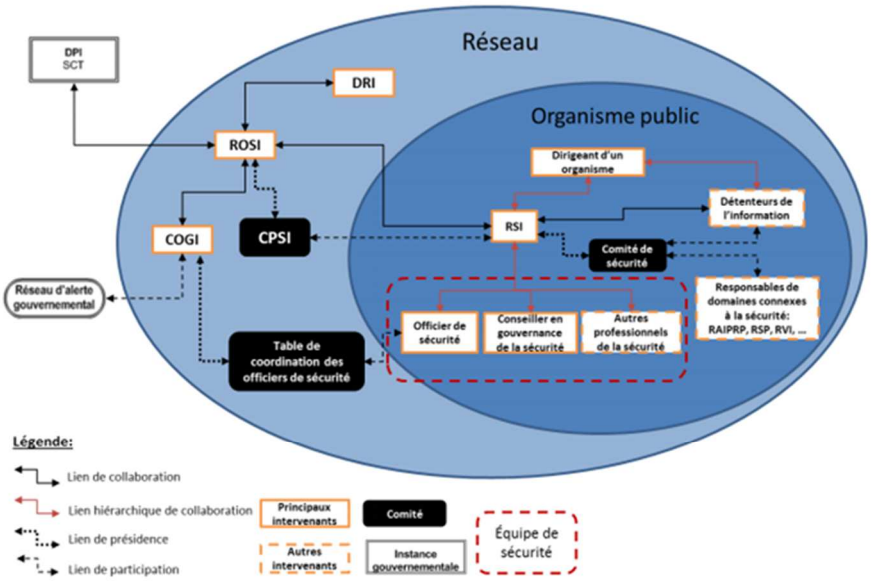


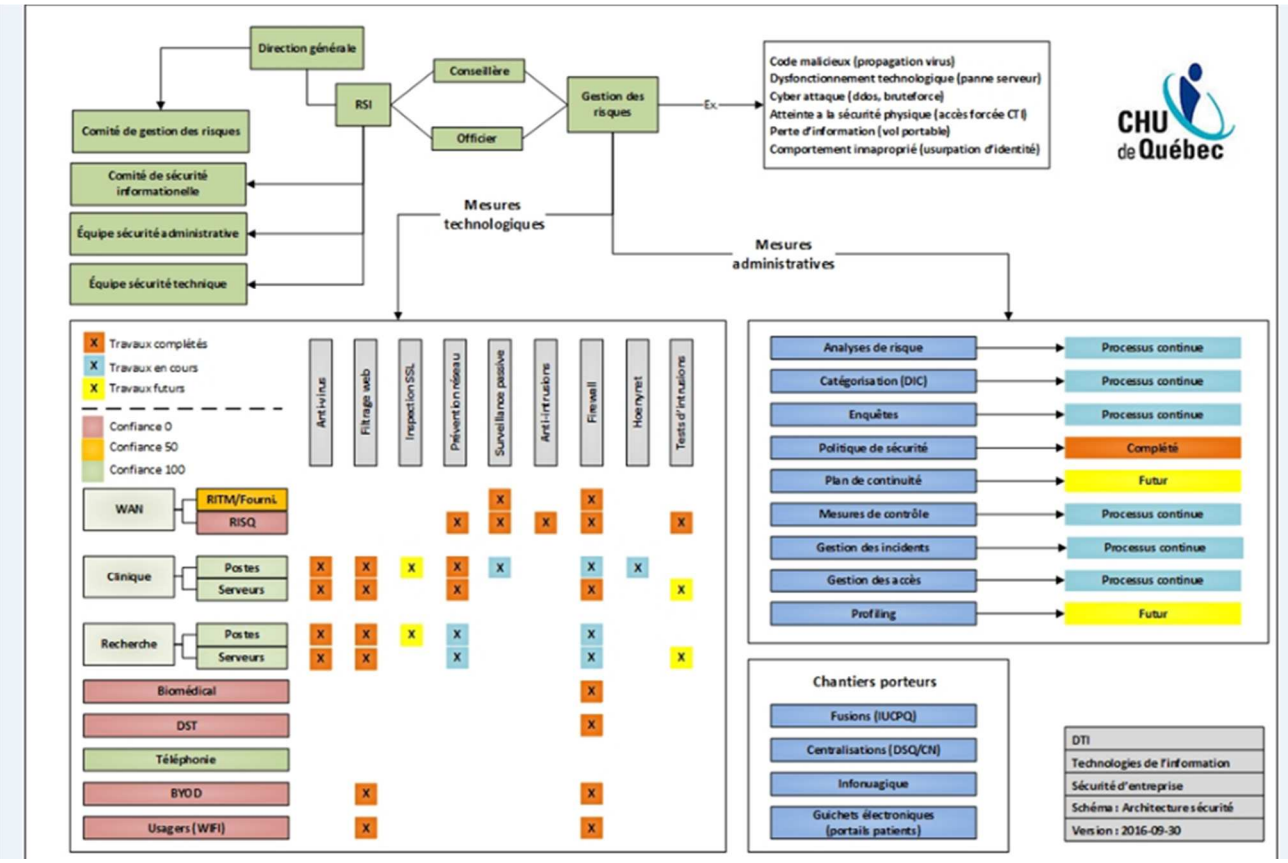
Figure 2: Structure fonctionnelle[4] de la sécurité de l'information du Réseau

[4] DPI: Dirigeant principal de l'information
DRI: Dirigeant réseau de l'information
ROSI: Responsable organisationnel de la sécurité de l'information
COGI: Coordonnateur organisationnel de la gestion des incidents
CPSI: Comité provincial de sécurité de l'information
RSI: Responsable de la sécurité de l'information
RAIPRP: Responsable de l'accès à l'information et de la PRP
RSP: Responsable de la sécurité physique
RVI: Responsable de la vérification interne

6. ARCHITECTURE DE SÉCURITÉ DE L'ÉTABLISSEMENT

L'architecture de sécurité de l'établissement comprend une vision commune et globale de l'ensemble des dimensions de l'établissement (affaires, organisationnelles et technologiques) en termes de sécurité. Cette vision doit être arrimée aux stratégies et aux processus d'affaires de l'établissement.

Concrètement, l'architecture de sécurité décrit l'ensemble des mesures de sécurité et permet d'y référer. Il contient généralement un inventaire des mesures, un schéma qui les représente, une planification et tous autres outils qui permettent de suivre et de faire évoluer la sécurité à un niveau global.



7. RÔLES ET RESPONSABILITÉS

7.1. Le conseil d'administration

- Adopte la politique et le plan d'action établis par l'établissement en matière de sécurité de l'information, lesquels sont conformes à la politique de sécurité de l'information et au cadre de gestion de la sécurité de l'information;

- Reçoit et entérine annuellement, ou au besoin, le bilan de sécurité de l'information de l'établissement.

7.2. Le dirigeant de l'organisme public

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

- 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;

- Approuve le cadre de gestion de la sécurité de l'information adapté à son établissement;

- S’assure de la mise en œuvre de la politique de sécurité de l’information adoptée par le conseil d’administration de même que du respect des rôles et des responsabilités définies dans le présent cadre de gestion de la sécurité de l’information;

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

- Établit, avec le responsable de la sécurité de l’information (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;

- Informe et mobilise ses gestionnaires et l’ensemble de son personnel au sujet de l’application des bonnes pratiques en matière de sécurité de l’information;

- S’assure de la gestion adéquate des risques de sécurité de l’information en lien avec son contexte organisationnel;

- S’assure de la nomination des détenteurs de la sécurité de l’information pour son établissement afin d’assurer la sécurité de l’information et des ressources qui la sous-entendent;

- S’assure de la mise en place d’un comité chargé de la sécurité de l’information au sein de son établissement et mandate le responsable de la sécurité de l’information pour présider ce comité.

7.3. Le responsable de la sécurité de l’information

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

- Planifie les activités nécessaires à la mise en place de la sécurité de l’information au sein de l’établissement;

- S’assure de l’encadrement de la sécurité de l’information au sein de l’établissement. Veille à l’application de la politique et du cadre de gestion de la sécurité de l’information et s’assure du respect des règles particulières publiées par le dirigeant réseau de l’information (DRI) en matière de sécurité de l’information;

- Agit à titre de porte-parole du responsable organisationnel de la sécurité de l’information (ROSI) auprès de l’établissement 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 œuvre;

- Représente son établissement au Comité provincial de la sécurité de l'information du Réseau et s'assure de la participation de son établissement aux processus provinciaux de gestion de la sécurité de l'information;

- Dirige la coordination et la cohérence des activités de sécurité de l'information menées au sein de l'établissement, notamment celles de son officier de sécurité de l'information et de son conseiller en gouvernance de la sécurité, le cas échéant;

- Préside, pour le compte du dirigeant de l'établissement, le comité de sécurité de l'information au sein de l'établissement 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'établissement, ainsi que toute proposition d'action ou d'état d'avancement des projets destinés au dirigeant de l'établissement;

- 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;

- S'assure de la mise en œuvre 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 établissement;

- S'assure de la mise en œuvre d'un processus de gestion des incidents de sécurité de l'information dans son établissement;

- 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;

- 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;

- Veille à la mise en œuvre de toute recommandation jugée pertinente découlant d'une vérification ou d'un audit de sécurité;

- S'assure de l'élaboration et de la mise en œuvre d'un programme formel de formation et de sensibilisation en matière de sécurité de l'information;

- S'assure de la production d'un bilan annuel ou, au besoin, d'un plan d'action triennal de la sécurité de l'information pour son établissement, le valide et le transmet au responsable organisationnel de la sécurité de l'information (ROSI) du Réseau et à son dirigeant d'établissement;

- Rend compte des réalisations de son établissement en matière de sécurité de l'information au responsable organisationnel de la sécurité de l'information (ROSI) du Réseau et à son dirigeant d'établissement;

- Évalue constamment toute information reçue en lien avec la sécurité de l'information.

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

7.4. Le conseiller en gouvernance de la sécurité de l'information

Le conseiller en gouvernance de la sécurité de l'information (CGSI) apporte son soutien au responsable de la sécurité de l'information (RSI) de son établissement, notamment en ce qui concerne l'encadrement de la sécurité de l'information, le choix des moyens pour rencontrer les exigences des règles particulières adoptées par le dirigeant réseau de l'information (DRI) et la planification des actions en sécurité. À cet égard, il :

- Accompagne le responsable de la sécurité de l'information (RSI) dans la définition des orientations stratégiques, des directives et des plans d'action en matière de sécurité de l'information;

- Participe à la rédaction des documents d'encadrement de la sécurité de l'information de son établissement, notamment la politique et le cadre de gestion de sécurité de l'information;

- Accompagne le responsable de la sécurité de l'information (RSI) dans la mise en œuvre des orientations internes découlant des directives ministérielles et celles du dirigeant réseau de l'information (DRI), des politiques internes et des pratiques généralement admises à cet égard;

- Participe à la définition des processus formels de gestion de la sécurité de l'information et accompagne le responsable de la sécurité de l'information (RSI) dans leur mise en œuvre;

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

- 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'établissement et pour le MSSS;

- 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;

- Élabore et met en œuvre le programme de formation et de sensibilisation en matière de sécurité de l'information;

- Tient à jour le registre d'autorité de la sécurité de l'information;

- Assure la coordination et la réalisation de projets de sécurité de l'information;

- Produit les bilans et les plans d'action de sécurité de l'information de son établissement.

7.5. L'officier de sécurité de l'information

L'officier de sécurité de l'information (OSI) est un professionnel de la sécurité de l'information ayant les compétences nécessaires à la réalisation des tâches et responsabilités suivantes. À ce titre, il :

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

- Participe activement au réseau d'alerte du Réseau pour la gestion des incidents de sécurité de l'information;

- Contribue aux analyses de risques de sécurité de l'information, identifie les menaces et les situations de vulnérabilité et met en œuvre les solutions appropriées;

- Supporte le responsable de la sécurité de l'information (RSI) et le conseiller en gouvernance de la sécurité de l'information (CGSI) 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;

- 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;

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

7.6. Le Comité de sécurité de l'information de l'établissement

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

- 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'établissement, ainsi que toute proposition d'action ou d'état d'avancement de projets en sécurité de l'information;

- S'assure de la prise en charge des risques, des situations vulnérables ou des incidents identifiés;

- Analyse et formule des recommandations concernant les événements ayant mis ou qui auraient pu mettre en péril la sécurité de l'information de l'établissement.

Ce comité est présidé par le responsable de la sécurité de l'information (RSI), à titre de représentant du dirigeant de l'établissement. 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, de toute personne jugée pertinente.

7.7. 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 :

- Communiquent au responsable de la sécurité de l'information (RSI) de l'établissement les problématiques et les préoccupations de sécurité en rapport avec leur domaine;
- Contribuent à assurer la cohérence et l'harmonisation des interventions en sécurité de l'information, y compris lors de la mise en œuvre du processus de gestion des risques et des incidents de sécurité de l'information;
- Participent au Comité de sécurité de l'information de l'établissement.

Au CHU de Québec-Université Laval, il s'agit du :

- Responsable de la gestion des technologies de l'information;
- Responsable de l'architecture d'entreprise, volet sécurité;
- Responsable de l'accès à l'information et de la protection des renseignements personnels;
- Responsable de la sécurité physique;
- Responsable de la gestion documentaire;
- Responsable de la continuité des services;
- Responsable de l'éthique;
- Responsable de la gestion de la qualité et des risques organisationnels.

7.8. Les détenteurs de l'information

Les détenteurs de l'information sont responsables d'assurer la sécurité des actifs informationnels qui leurs sont confiés par le dirigeant de l'établissement. Notamment, ils :

- S'impliquent dans l'ensemble des activités relatives à la sécurité, soit 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;
- S'assurent de connaître et d'évaluer les risques et les vulnérabilités de leurs actifs informationnels, priorisent les actions correctives appropriées et gèrent leur application selon le plan d'action déterminé;
- S'assurent que les mesures de sécurité appropriées sont élaborées, approuvées, mises en place et appliquées systématiquement;

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

- Déterminent les règles d'accès aux actifs informationnels dont ils assument la responsabilité avec l'appui du responsable de la sécurité de l'information (RSI) de l'établissement.

7.9. Les gestionnaires

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

- 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 œuvre. De plus, ils les sensibilisent à la nécessité de s'y conformer;

- S'assurent que les actifs informationnels mis à la disposition de leur personnel sont utilisés en conformité avec les principes généraux, les exigences de sécurité de l'information et les règles particulières;

- 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 les règles de sécurité de l'information de l'établissement.

7.10. Les utilisateurs

Les utilisateurs dûment autorisés à accéder aux actifs informationnels de l'établissement :

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

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

7.11. Le responsable des processus de soutien en sécurité (RPSS)

Ce poste ne fait pas partie des exigences gouvernementales. Il est présenté spécifiquement pour le CHU de Québec-Université Laval afin d'avoir un cadre de gestion complet démontrant les équipes de soutien aux opérations. La personne désignée est le chef de service de la Direction des technologies de l'information du CHU de Québec-Université Laval. À ce titre, il :

- S'assure que les mécanismes de suivi et de contrôle sont adéquatement utilisés;

- Prend en charge l'application des mesures de sécurité décrétées par l'établissement;

- Soulève tout manquement à la sécurité et participe activement à proposer des solutions de redressement ou d'amélioration;

- Agit à titre de conseiller auprès des responsables des services ou des demandeurs en tenant compte des normes et des standards selon les meilleures pratiques en technologies de l'information;

- Participe à l'élaboration des méthodes alternatives de gestion de l'informatique en cas d'arrêt des systèmes informatisés, en partenariat avec sa clientèle;

- Collabore à l'élaboration des procédures de gestion relatives au traitement de l'information, et à celles reliées à l'accès, à la protection et à la conservation des données;

- Collabore au maintien de la sécurité et de la confidentialité des données, conformément au *Cadre global de gestion des actifs informationnels*;

- Assure la conformité des architectures technologiques avec les orientations technologiques du MSSS;

- Voit à l'application des normes et des standards de sécurité en vigueur dans le Réseau.

Le responsable des processus de soutien en sécurité (RPSS) gère les équipes en sécurité de l'information et en technologies. La structure organisationnelle est composée des 5 secteurs suivants :

- Téléphonie;

- Réseautique;

- Télécommunications et sécurité;

- Bureau d'analyse des processus de soutien et de contrôle;

- Centre de traitement informatique;

- Analystes en informatique.

7.12. Réseautique et télécommunications

Le secteur réseautique regroupe l'ensemble des activités visant à assurer la disponibilité et le bon fonctionnement des liens et des télécommunications de façon transparente entre les utilisateurs et les technologies informatiques, et ce, en étant à l'affût des nouveautés afin d'innover et d'être proactif dans le but de permettre l'évolution du CHU de Québec-Université Laval. Les activités réalisées sont les suivantes :

- Assurer la sécurité et la stabilité de l'infrastructure de télécommunication informatique;

- Assumer la responsabilité de l'analyse, de la maintenance et de la surveillance des réseaux informatiques;

- Gérer et opérer les réseaux de communication, de téléphonie et de vidéoconférence;

- Être responsable de la stabilité des communications de données et de voie (filaire ou sans-fil);
- Veiller à la conception des architectures de réseau, élabore et met en application des solutions aux défaillances des systèmes et des réseaux informatiques.

7.13. Sécurité technique et base de données

Le secteur télécommunications et sécurité regroupe l'ensemble des activités visant à assurer la sécurité du périmètre, la stabilité et la récupération des bases de données, puis la surveillance proactive des systèmes informatisés du CHU de Québec-Université Laval. Les activités réalisées sont :

- Veiller à la gestion et à l'exploitation des données et des logiciels des bases de données;
- Gérer de façon centralisée l'antivirus, les anti-spam et les mises à jour Microsoft;
- Définir et implémenter les stratégies d'accès distant;
- Mettre en place les infrastructures de sécurité optimales et ajuster des dispositifs de sauvegarde et de restauration des bases de données;
- Administrer les coupe-feux, les serveurs mandataires (proxys) et les systèmes de prévention d'intrusion (IPS);
- Élaborer les stratégies d'accès et d'audit d'Internet.

7.14. Bureau d'analyse des processus de soutien et de contrôle

Le secteur du bureau d'analyse des processus de soutien et de contrôle regroupe l'ensemble des activités visant à assurer la mise en place, la maintenance et la stabilité des environnements informatiques applicatifs du CHU de Québec-Université Laval. Il met en place la documentation et les processus d'assistance technique. Les activités réalisées sont :

- Veiller à la qualité des produits et des services selon les standards, les normes et les procédures à suivre;
- Gérer la mise en place des nouveaux logiciels ainsi que des mises à niveaux ultérieures;
- Émettre et appliquer des solutions aux défaillances informatiques;
- Mettre en place les procédures d'installation et de configuration;
- Rédiger la documentation technique complète des applications.

7.15. Centre de traitement informatique

Le secteur du centre de traitement informatique regroupe l'ensemble des activités visant à assurer une disponibilité et une utilisation optimale des différents systèmes d'information du CHU de Québec-Université Laval. Le centre de traitement informatique permet d'assurer la configuration logicielle et matérielle des serveurs, des environnements d'entreposage (SAN) et des engins de

sauvegarde. Il permet aussi d'assurer l'évolution des composantes technologiques des différents systèmes en participant à l'évaluation et à l'élaboration de projets technologiques. Les activités réalisées sont :

- Supporter et administrer tous les serveurs (physiques et virtuels);
- Être responsable des infrastructures de stockage de données;
- Être responsable des processus de relève des systèmes en technologies de l'information;
- Assurer l'installation et le remplacement des serveurs physiques et virtuels.

7.16. Centre d'assistance, service de proximité

- Collabore à l'élaboration des procédures de gestion relatives au traitement de l'information, et à celles reliées à l'accès, à la protection et à la conservation des données;
- Collabore au maintien de la sécurité et de la confidentialité des données, conformément aux normes ministérielles.

7.17. Bureau de projet

- Collabore au maintien de la sécurité et de la confidentialité des données, conformément aux normes ministérielles;
- Soutient la mise en place des processus de sécurité dans les projets.

7.18. Télésanté

- Anticipe et évalue, par une vigie continue des technologies, les solutions nouvelles en lien avec les cibles technologiques et d'affaires, porte une appréciation sur leur degré de maturité et analyse l'impact d'intégration dans l'établissement;
- Assure la conformité des architectures technologiques avec les orientations technologiques du MSSS;
- Voit à l'application des normes et des standards de sécurité en vigueur dans le Réseau.

8. ENTRÉE EN VIGUEUR

Le présent cadre de gestion entre en vigueur le jour de son adoption par la présidente directrice générale de l'établissement.

9. RÉFÉRENCES

Le CHU de Québec-Université Laval s'est appuyé notamment sur la *Politique provinciale de la sécurité de l'information* et sur le *Cadre de gestion de la sécurité de l'information* daté d'août 2015 pour rédiger le présent document.

10. DISPOSITIONS FINALES

Le présent cadre de gestion entre en vigueur à la date de son approbation par la présidente-directrice générale de l'établissement. À compter de cette date, l'établissement doit procéder à son application dans les délais prescrits. Le cadre de gestion doit être réévalué à chaque modification de la politique de sécurité de l'information et à l'occasion de changements organisationnels ou de nouvelles orientations ministérielles.