AGENCE DE LA SANTÉ ET DES SERVICES SOCIAUX DE MONTRÉAL | vivre une île en santé

BILAN DE LA SÉCURITÉ DES ACTIFS INFORMATIONNELS 2013-2015

DE L'AGENCE DE LA SANTÉ ET DES SERVICES SOCIAUX DE MONTRÉAL

Québec

BILAN DE LA SÉCURITÉ DES ACTIFS INFORMATIONNELS 2013-2015

DE L'AGENCE DE LA SANTÉ ET DES SERVICES SOCIAUX DE MONTRÉAL

Approuvé par le conseil d'administration du 30 mars 2015.

Agence de la santé et des services sociaux de Montréal
Québec

Coordination
Loraine Desjardins, adjointe à la direction générale

Recherche et rédaction
Stéphane Gagnon, CISSP, responsable de la sécurité des actifs informationnels

Merci aux membres du Comité sur la sécurité des actifs informationnels (CSAI) de l'Agence de la santé et des services sociaux de Montréal pour leur collaboration à la production et à la validation des informations

Ce document a été réalisé avec la collaboration de Florence Mancel, agente administrative

Production
Direction générale de l'Agence de la santé et des services sociaux de Montréal
Mars 2015

Bilan de la sécurité des actifs informationnels 2013-2015

ISBN 978-2-89510-830-6 (version imprimée)
ISBN 978-2-89510-831-3 (PDF)

Dépôt légal - Bibliothèque et Archives nationales du Québec, 2015

Ce document est disponible :
au centre de documentation de l'Agence : 514 528-2400 poste 3268
à la section «Publications de l'Agence» du site Internet : http://agence.santemontreal.qc.ca/

TABLE DES MATIÈRES

ACRONYMES ET DÉFINITIONS 5

PRÉAMBULE 6

1. Contexte 7

2. Intervenants de l'Agence en sécurité des actifs informationnels 9

3. Statut sur les recommandations du plan d'ACTION 2013-2015 10

4. Bilan 2013-2015 des activités 14

3.1 Participation à la mise en place du filtrage Web pour la région de Montréal 14

3.2 Mise à jour des risques majeurs touchant l'Agence 14

3.3 Rédaction d'une politique de mots de passe 15

3.4 Réalisation d'un audit interne sur l'implantation des 15 mesures prioritaires du Cadre global 15

3.5 Discussion sur le chiffrement des données cliniques 16

3.6 Rencontre avec les cadres de la direction des technologies et systèmes d'information (DTSI) concernant le plan de continuation des affaires et du plan de relève 16

3.7 Analyse des accès avec les jetons de téléaccès 16

3.8 Achat d'un logiciel d'analyse de vulnérabilités 16

3.9 Rédaction d'une politique de gestion du filtrage Web 16

3.10 Rencontre avec l'auditeur externe 16

3.11 Préparation du bilan de sécurité selon le gabarit produit par le Ministère de la Santé et des services sociaux du Québec (MSSS) 17

3.12 Directive concernant le cadre de gestion de la sécurité de l'information produit par le Ministère de la Santé et des services sociaux du Québec (MSSS) 17

3.13 Essai d'un programme de sensibilisation à la sécurité de l'information offert par le centre de service partagés du Québec (CSPQ) 17

3.14 Réalisation d'une première analyse de vulnérabilités (Site St-Denis et Pavillon Lafontaine) 17

3.15 Réalisation d'une première analyse de vulnérabilités (Technocentre) 17

3.16 Conseils sur différents projets technologiques de l'Agence 18
3.17 Intérim à coordination régionale de la sécurité des actifs informationnels pour la région de Montréal (CRSAI) 18
3.18 Sensibilisation du personnel de l'Agence 18
3.19 Rencontres du Comité de sécurité des actifs informationnels (CSAI) 18

5. Plan d'action 2015-2016 20

6. Conclusion 22

7. LISTE DES ANNEXES 23
Annexe 1 – Rôles des intervenants/entités à l'Agence dans la protection des actifs informationnels 24
Annexe 2 -15 mesures prioritaires du Cadre global 27
Annexe 3 – Recommandations suite à l'audit interne croisé des 16 et 17 octobre 2013 29
Annexe 4 – Composition et mandats du comité de sécurité des actifs informationnels (CSAI) 30

ACRONYMES ET DÉFINITIONS

Actifs informationnels (AI)	C'est une banque d'information électronique, système d'information, réseau de télécommunications, technologie de l'information, installation ou ensemble de ces éléments ; un équipement médical spécialisé ou ultra spécialisé peut comporter des composantes qui font partie des actifs informationnels, notamment lorsqu'il est relié de façon électronique à des actifs informationnels. (réf. : Loi sur les services de santé et les services sociaux, art.520.1). S'ajoutent, dans le présent cadre de gestion, les documents imprimés générés par les technologies de l'information.
Audit interne croisé	Vérification réalisée par les ressources internes de l'Agence pour s'assurer de notre conformité aux 15 mesures prioritaires du cadre global.
CGGAI (Cadre global de gestion des Actifs informationnels)	Appelé aussi Cadre global Document produit par le MSSS qui encadre et régit l'utilisation des actifs informationnels dans le réseau de la santé et des services sociaux.
CIUSSS	Centre intégré universitaire de santé et services sociaux
CRSAI	Coordonatrice régionale de la sécurité des actifs informationnels
DIC	Disponibilité, Intégrité et Confidentialité (les 3 principes fondamentaux en sécurité de l'information)
DTSI	Direction des technologies et des systèmes d'information
DAIRH	Direction des affaires institutionnelles et des ressources humaines
DSP	Direction de la santé publique
Filtrage internet	Outil de surveillance et de contrôle d'accès aux sites internet
RSAI	Responsable de la sécurité des actifs informationnels. S'assure de la mise en œuvre de diverses activités encadrant la sécurité des actifs informationnels telle que stipulée dans le cadre global du MSSS
RSSS	Réseau de la santé et des services sociaux
TCR	Le Technocentre régional de Montréal

PRÉAMBULE

Le présent bilan sur la sécurité des actifs informationnels de l'Agence de la santé et des services sociaux de Montréal (ASSSM) est présenté pour une seconde année au conseil d'administration et couvre la période 2013-2014. Il s'agit du dernier bilan de sécurité produit par l'ASSSM étant donné l'avènement du projet de loi n°10 : Loi modifiant l'organisation et la gouvernance du réseau de la santé et des services sociaux notamment par l'abolition des agences régionales (PL-10).

Après un premier dépôt en 2011, le présent bilan démontre que l'Agence bénéficie d'une protection adéquate de base pour l'ensemble de ses actifs. Cependant, certaines améliorations devraient être apportées à court terme afin de conserver un niveau de protection efficace.

En matière de sécurité des actifs informationnels, les agences de santé et services sociaux sont considérées comme des établissements. Elles sont donc soumises aux mêmes lois et règlements et doivent ainsi se conformer aux préceptes qui encadrent la sécurité des actifs informationnels.

Le document propose une brève analyse du contexte qui permet de situer l'encadrement législatif ainsi que l'importance du cadre global qui régissent le domaine de la sécurité des actifs informationnels.

Il décrit les réalisations et les mesures qui ont été implantées par les équipes de l'Agence au cours de la période 2013-2015 afin de protéger ses actifs informationnels sur les quatre sites physiques qu'elle occupe actuellement.

Le document contient également une série de 22 recommandations provenant de quatre sources pour lesquelles des actions ont déjà été réalisées et d'autres qui seront faites en cours d'année.

Un plan d'action et des pistes d'amélioration pour mieux limiter les risques reliés à la sécurité terminent ce bilan.

Une série d'annexes vient compléter l'information contenue dans le présent document.

Un actif informationnel est une banque d'information électronique, système d'information, réseau de télécommunications, technologie de l'information, installation ou ensemble de ces éléments; un équipement médical spécialisé ou ultra spécialisé peut comporter des composantes qui font partie des actifs informationnels, notamment lorsqu'il est relié de façon électronique à des actifs informationnels. S'ajoutent, dans le présent cadre de gestion, les documents imprimés générés par les technologies de l'information.

(réf. : Loi sur les services de santé et les services sociaux, art.520.1)

1. CONTEXTE

La sécurité des actifs informationnels est une préoccupation majeure des intervenants œuvrant dans le domaine de la santé et des services sociaux. L'information et les données contenues dans ces actifs informationnels sont essentielles aux activités courantes des utilisateurs et présentent une valeur clinique, légale, administrative et financière irremplaçable. À ce titre, celles-ci doivent faire l'objet d'une utilisation appropriée et d'une protection adéquate. Les mesures de sécurité sont donc applicables à toute information, que ce soit des renseignements personnels, des données cliniques, financières ou administratives sur support électronique ou papier.

Cadre global

C'est pourquoi le ministère de la Santé et des Services sociaux a officialisé en septembre 2002 le **« Cadre global de gestion de la sécurité des actifs informationnels appartenant aux organismes du réseau de la santé et des services sociaux — Volet sur la sécurité »**, ci-après intitulé le Cadre global.

Encadrement législatif

Le Cadre global prend en considération l'ensemble des lois, des codes d'éthique, des codes déontologiques et des pratiques actuellement appliqués en matière de transmission de l'information sur les usagers. Il intègre tant l'information de nature clinique que celles de nature administrative et clinico-administrative.

Les lois et directives qui encadrent et régissent l'utilisation de l'information :

- La Loi sur les services de santé et les services sociaux (L.R.Q., c. S-4.2),
- La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1).
- Le Code civil (art. 35 et 41).
- La Loi sur les archives (L.R.Q., c. A-21.1).
- Le document produit par la Commission d'accès à l'information en 1992, intitulé : «*Exigences minimales relatives à la sécurité des dossiers informatisés des usagers du RSSS* ».

De plus, une nouvelle directive gouvernementale portant sur la sécurité de l'information est entrée en fonction depuis janvier 2014. Celle-ci apporte de nombreux changements au niveau de la gestion de la sécurité de l'information. Cette directive provient de la loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (L.R.C. c. G-1.03).

Particularités de l'Agence de Montréal

L'Agence de Montréal regroupe 4 installations physiques différentes. Cette situation demande d'harmoniser les outils de collecte des informations et les mesures à prendre pour assurer la sécurité des actifs informationnels de façon uniforme.
Les quatre sites de l'Agence sont :

1- L'Agence de la santé et des services sociaux de Montréal
2- La Direction de santé publique
3- Le Technocentre régional (2 installations)

Il existe donc une variété de mesures qui sont appliquées afin de s'assurer de bien utiliser et de protéger adéquatement l'information qui fait partie des opérations courantes des utilisateurs de l'Agence de Montréal dans ses différents sites.

Gestion de la sécurité des actifs informationnels

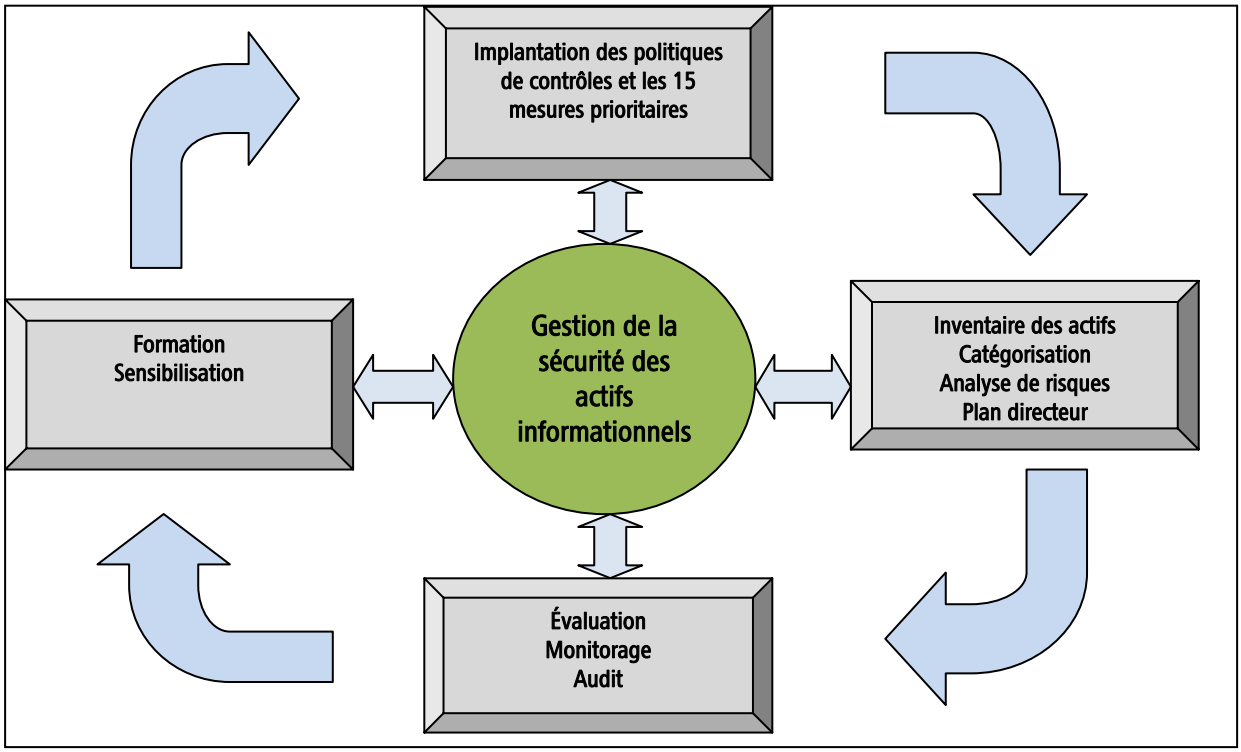

Fig. 1 Gestion de la sécurité des actifs informationnels

2. INTERVENANTS DE L'AGENCE EN SÉCURITÉ DES ACTIFS INFORMATIONNELS

La sécurité des actifs informationnels comporte plusieurs enjeux – qu'ils soient d'ordre organisationnel, professionnel, économique, technologique, politique, éthique ou légal. Les mesures visant à assurer cette sécurité intéressent plus que jamais aussi bien les hautes instances gouvernementales que les gestionnaires, les spécialistes et le personnel du système de santé ainsi que toute personne ayant accès aux renseignements personnels et aux autres informations numériques. La gestion de la sécurité des actifs informationnels devient une préoccupation partagée par tous les acteurs concernés par cette question. Le tableau ci-dessous précise les intervenants impliqués dans la chaîne de la sécurité des actifs informationnels.

Intervenant/entité
Conseil d'administration (CA)
Présidente-directrice générale (PDG)
Comité de la sécurité des actifs informationnels (CSAI)
Responsable de sécurité des actifs informationnels (RSAI)
Direction des technologies et systèmes d'information (DTSI)
Gestionnaires et détenteurs des actifs
Direction des affaires institutionnelles et des ressources humaines (DAIRH)
Utilisateurs

La liste détaillée des différents acteurs ainsi que leurs rôles en lien avec la protection des actifs informationnels se trouvent à l'annexe 1 du présent document

3. STATUT SUR LES RECOMMANDATIONS DU PLAN D'ACTION 2013-2015

Les actions de sécurité prévues à l'Agence pour l'année 2013-2015 sont énumérées ci-dessous avec le statut de réalisation de celles-ci. Plusieurs recommandations ont été mises en place, d'autres n'ont pas été réalisées à cause d'un changement de contexte (déménagement, légal, etc.). Certaines recommandations seront de retour dans le prochain bilan.

	Recommandation	Action	Statut
R.1.	Identifier le journal du système d'exploitation permettant d'identifier les accès et les tentatives infructueuses (Pavillon Lafontaine)	Mettre en place un outil permettant d'identifier dans les journaux d'événements les accès et les tentatives infructueuses	Complétée
R.2.	Mettre en place un programme de sensibilisation à la sécurité des actifs informationnels pour le personnel des technologies de l'information	Développer un programme de sensibilisation spécifique au personnel travaillant en technologie de l'information	Complétée Suivi reste à faire
R.3.	Prévoir un mécanisme de protection pour les ordinateurs portatifs ainsi que les appareils mobiles	Rechercher les différents mécanismes disponibles permettant la protection des données contenues sur le disque rigide des appareils portatifs ainsi que sur les appareils mobiles	Non complétée Pas priorisé
R.4.	Remplacer le registre papier par un système à carte magnétique pour plus d'imputabilité (Siège social et Pavillon Lafontaine)	Évaluer les coûts liés à l'ajout d'un lecteur de carte magnétique pour le siège social et la Pavillon Lafontaine Faire l'analyse du risque sachant que les actifs critiques sont déplacés vers le Technocentre versus les coûts liés à l'ajout d'un lecteur de carte magnétique	N'est plus d'actualité en raison de la migration de nombreux actifs informationnels au Technocentre régional de Montréal et l'éventuel déménagement des employés du Pavillon Lafontaine.
R.5.	Effectuer une vérification bisannuelle de l'inventaire des logiciels installés	Mettre en place un processus formel de gestion des licences (Acquisition, installation, désinstallation, etc.) Mettre en place un système d'extraction (liste) des logiciels installés sur les ordinateurs et implanter un processus de contrôle biannuel	Complétée

	Recommandation	Action	Statut
R.6.	Installer des gicleurs dans la salle des serveurs (Pavillon Lafontaine)	Faire l'analyse du risque sachant que les actifs critiques sont déplacés vers le Technocentre versus investir dans la salle en décroissance	N'est plus d'actualité
R.7.	Établir un bilan des mesures en place en matière de sécurité de l'information à l'Agence et dans les établissements	Déposer au conseil d'administration de l'Agence le bilan annuel 2011-2013	Complétée
R.8.	Participer à l'élaboration et à la mise en place du réseau d'alerte en sécurité de l'information au niveau de l'Agence et des établissements suivant les directives qui seront transmises	Définir un processus d'alerte en sécurité de l'information suivant les directives ministérielles avec les différents intervenants pouvant être impliqués lors d'un incident touchant la sécurité des actifs informationnels de l'Agence	Reportée par le MSSS
R.9.	Revoir l'accès des différents fournisseurs aux actifs informationnels de l'Agence	Mettre en place une politique de gestion des accès aux fournisseurs qui va appuyer une directive interne déjà existante au Technocentre	Complétée Suivi à faire
R.10.	Mettre en place un plan de relève informatique au Technocentre	Procéder à l'analyse afin d'élaborer un plan de relève informatique pour le Technocentre Relève de certaines applications est déjà en place (Oacis, Imagerie médicale)	Non complétée Des travaux ont débutés avec l'embauche d'un consultant à cet effet.
R.11.	Surveiller les équipements (applications, matériels et logiciels)	Poursuivre l'implantation de l'outil de journalisation syslog-ng au Technocentre régional de Montréal sur les équipements de type Windows	Abandonnée Il existe des outils sur le marché de type corrélateur d'événements pouvant faire le même travail.
R.12.	Surveiller l'utilisation de la bande passante et l'accès aux sites malveillants	Procéder à l'implantation du système de filtrage web régional sur les postes informatique de tous les sites de l'Agence d'ici la fin du mois de juin. Dans un premier temps, filtrage uniquement des accès aux sites malveillants Uniformiser la politique d'utilisation de l'internet à l'Agence et la faire approuver par le comité de direction pour un meilleur contrôle de la bande passante ainsi que l'accès aux sites malveillants	Complétée Il faut mentionner que l'accès aux sites malveillants est bloqué au niveau de la DGTI-MSSS à Québec.
R.13.	Établir une vigie sur les	Surveiller durant la prochaine année :	Complétée et doit se

	Recommandation	Action	Statut
	meilleurs pratiques en sécurité informatique	Le « BYOD » (« Bring Your Own Device »). Un utilisateur peut utiliser son ordinateur, téléphone intelligent ou tablette personnelle sur le réseau informatique de l'entreprise ; Les téléphones intelligents, tablettes doivent bénéficier de couches de protection supplémentaire ; • Le recours au chiffrement des données ; • La diversité des plates-formes et des technologies cause de nouvelles opportunités d'attaques ; Les risques affectant les actifs informationnels proviennent également de l'intérieur de l'entreprise (principalement de l'erreur humaine).	poursuivre
R.14.	Créer des divisions logiques sécurisées entre les projets	Limiter les accès logiques aux équipements situés dans la salle informatique du Technocentre	Partiellement complétée et doit se poursuivre
R.15.	Appliquer les mises à jour aux logiciels spécifiés suite au test d'intrusion	Installer les correctifs nécessaires aux logiciels spécifiés afin de corriger les différentes vulnérabilités	Complétée
R.16.	Harmoniser et diffuser une politique de mots de passe	Rédiger une politique sur la gestion des mots de passe	Partiellement complétée et doit se poursuivre Une première version de la politique fut rédigée et présenté aux membres du comité de sécurité des actifs informationnels (CSAI) à des fins de discussion
R.17.	Mettre en place une procédure formelle de révision périodique des comptes utilisateurs et de leurs privilèges d'accès aux applications (GRF, GRH et GRM)	Ajouter l'application GRF et GRM au processus annuel de révision des accès aux applications	Complétée
R.18.	Réviser les accès d'administrateurs de domaine afin que chaque compte est nominatif et nécessaire aux opérations	Mettre en place un processus de révision de la liste des codes d'utilisateurs ayant les privilèges d'administration du réseau informatique au siège social	Complétée
R.19.	Approbation des privilèges d'accès aux applications et la révision de ceux-ci devraient	Élaborer un processus de travail d'ici le 31 mars 2014 qui permettra de documenter les approbations et la révision des	Complétée

	Recommandation	Action	Statut
	être effectués par une personne distincte n'ayant pas les privilèges de gestion	privilèges afin que les opérations soient effectuées dans le système sur une base régulière par une personne distincte. Nous ne sommes pas en mesure compte tenu de la taille de l'équipe d'enlever les privilèges de gestion au gestionnaire responsable des approbations.	
R.20.	Activer les accès d'un fournisseur seulement lorsqu'une demande est approuvée par l'informatique conjointement avec le Technocentre	Arrimer cette recommandation avec celle concernant l'accès des différents fournisseurs aux actifs informationnels de l'Agence	Complétée Suivi reste à faire
R.21.	Configurer, lorsque possible, les paramètres de sécurité des applications (GRH et GRF) de manière à respecter la directive de gestion des mots de passe et aussi restreindre l'accès aux personnes autorisées	Effectuer une analyse d'impact préalable à la mise en place est requise Activer les paramètres qui permettent d'utiliser les codes d'utilisateurs du répertoire d'entreprise (Active Directory) qui respecte les exigences concernant les mots de passe Arrimer ce point avec les politiques de sécurité d'accès établis à l'Agence	Complétée
R.22.	Définir une entente de services stipulant les prestations à fournir, les modalités et les responsabilités de chaque partie devrait être discutée et formalisée avec le Technocentre	Négocier et signer une entente de service afin de définir les services à fournir, les modalités et responsabilités de chaque partie impliquée	Abandonnée Les équipes informatiques de l'Agence ont intégrées sous la même direction et le besoin de définir des ententes de service n'est plus nécessaire.

4. BILAN 2013-2015 DES ACTIVITÉS

Plusieurs activités ont été réalisées cette année afin d'améliorer la sécurité des actifs informationnels de l'Agence. Certaines d'entre-elles prennent la forme de rencontres avec des équipes de projets, des réponses à des interrogations sur les aspects touchant la sécurité des actifs et des mesures de protection à mettre en place.

Année	Réalisations
Avril 2013	Participation à la mise en place du filtrage Web pour la région de Montréal
Avril 2013	Mise à jour des risques majeurs de l'Agence
Juillet 2013	Rédaction d'une politique de mots de passe
Octobre 2013	Réalisation d'un audit interne sur l'implantation des 15 mesures prioritaires du Cadre global
Octobre 2013	Discussion sur le chiffrement des données cliniques
Novembre 2013	Rencontre avec les cadres de la Direction des technologies et systèmes d'information (DTSI) concernant le plan de continuation des affaires et du plan de relève
Janvier 2014	Analyse des accès avec les jetons de téléaccès
Janvier 2014	Achat d'un logiciel d'analyse de vulnérabilités
Février 2014	Rédaction d'une politique de gestion du filtrage Web
Février 2014	Rencontre avec l'auditeur externe
Mars 2014	Préparation du bilan de sécurité selon le gabarit produit par le Ministère de la Santé et des Services sociaux du Québec (MSSS)
Mars 2014	Directive concernant le cadre de gestion de la sécurité de l'information
Mars 2014	Essai d'un programme de sensibilisation à la sécurité de l'information (offert par le Centre de service partagé du Québec)
Mars 2014	Réalisation d'une première analyse de vulnérabilités (Site DSP et St-Denis)
Mai 2014	Réalisation d'une première analyse de vulnérabilités (Technocentre)
2013-2015	Conseils sur différents projets technologiques de l'Agence
2014-2015	Intérim à la coordination régionale de la sécurité des actifs informationnels pour la région de Montréal
Mars 2015	Dépôt du bilan annuel de la sécurité des actifs informationnels 2013-2014

3.1 Participation à la mise en place du filtrage Web pour la région de Montréal

Le RSAI a été impliqué dans ce projet sur les aspects touchant la sécurité des actifs. Par exemple, sur le choix des différentes catégories des sites Web autorisés ou bloqués, la redondance des équipements de filtrage en cas de panne et l'utilisation des rapports afin de pouvoir auditer l'utilisation d'Internet par les employés de l'Agence afin que la politique de sécurité des actifs informationnels soit respectée.

3.2 Mise à jour des risques majeurs touchant l'Agence

En avril 2013, le MSSS demandait aux agences une analyse des risques majeurs afin de produire un plan d'action. Cet exercice a démontré que la majorité des équipes consultées à l'Agence percevait les risques liés à la gestion et à la sécurité des actifs informationnels comme prioritaires et critiques.

Les principaux risques identifiés :

- la sécurité des données;

- la pérennité des actifs technologiques;
- les intrusions à son réseau informationnel;
- les fuites de renseignements;
- l'absence d'un plan de relève au Technocentre.

Le tableau suivant présente les mesures réalisées afin d'atténuer ou éliminer ces risques.

Risques	Mesures atténuantes
Sécurité des données	Participation accrue du RSAI dans le processus d'implantation des nouveaux projets. Révision de la sécurité dans l'infrastructure informatique.
Intrusion à son réseau informationnel	Processus de mise en place des divisions logiques sécurisées entre les projets.
Fuite de renseignements	Mise en place des recommandations suite au test d'intrusion réalisé au Technocentre. Plusieurs recommandations suite au test d'intrusion peuvent être mises en place sur l'ensemble des installations de l'Agence.
Absence d'un plan de relève au Technocentre	Mise en place d'une infrastructure de relève pour les applications critiques hébergées au Technocentre. Embauche d'un consultant afin d'élaborer un plan de relève.

3.3 Rédaction d'une politique de mots de passe

L'utilisation des mots de passe est très souvent le seul moyen utilisé afin de valider l'identité d'un utilisateur (authentification). L'objectif est de mieux définir les normes à respecter en matière de mots de passe. De nombreuses failles informatiques proviennent de mots de passe qui ont un niveau de sécurité insuffisant.

3.4 Réalisation d'un audit interne sur l'implantation des 15 mesures prioritaires du Cadre global

L'Agence poursuit la validation de l'implantation des 15 mesures prioritaires du Cadre global de la sécurité des actifs informationnels appartenant aux organismes du réseau de la santé et des services sociaux – volet sécurité (CGGAI-VS) (voir l'annexe 2 pour les détails des 15 mesures).

En octobre 2013, un troisième audit interne a été réalisé sur l'ensemble des installations de l'Agence afin de valider l'atteinte des exigences liées à l'implantation de ces mesures. Pour ce faire, un comité a été formé composé des auditeurs suivants : Mme Louise Francoeur (analyste informatique, Pavillon Lafontaine), M. André Côté (analyste informatique, Saint-Denis) et M. Stéphane Durand (Chef de service (SYSCOR) - deux installations du Technocentre) ainsi que M. Stéphane Gagnon (responsable de la sécurité des actifs informationnels).

Lors de ce processus, des questions de base ont été posées et certaines preuves demandées aux fins de vérification. Un rapport a été déposé, accompagné de recommandations (voir l'annexe 3 pour le détail des recommandations) pour chaque site afin de corriger les lacunes identifiées. Un tel exercice est effectué une fois par an.

3.5 Discussion sur le chiffrement des données cliniques

Le chiffrement des données cliniques permet d'assurer la confidentialité de celles-ci lorsque les informations sont échangées ou stockées sur des équipements informatiques. Des rencontres ont eu lieu avec certains fournisseurs et responsables d'applications afin d'envisager la possibilité de chiffrer les données cliniques hébergées à l'Agence (plus précisément au Technocentre régional de Montréal).

3.6 Rencontre avec les cadres de la direction des technologies et systèmes d'information (DTSI) concernant le plan de continuation des affaires et du plan de relève

Un atelier de discussions a eu lieu avec les cadres de la DTSI concernant la nécessité d'avoir un plan de continuation des affaires ainsi qu'un plan de relève pour le Technocentre régional de Montréal. Un consultant a également été embauché afin d'enclencher la démarche de réalisation des différents plans.

3.7 Analyse des accès avec les jetons de téléaccès

Il a été soulevé à l'attention du RSAI que plusieurs jetons de téléaccès demandés par les établissements du réseau montréalais de la santé avaient de nombreux accès (plus que suffisant) pour les actifs informationnels accédés par les utilisateurs.

Il y a eu un processus d'analyse des accès afin de restreindre les accès aux actifs. Un profil d'utilisateur spécifique a été créé afin de restreindre les accès.

3.8 Achat d'un logiciel d'analyse de vulnérabilités

Un logiciel d'analyse de vulnérabilités a été acheté par l'Agence. Ce logiciel permet de détecter des vulnérabilités pouvant se retrouver sur différents équipements informatiques (serveurs, applications, équipement de télécommunication). Ces mêmes vulnérabilités peuvent être exploitées par des personnes malveillantes afin d'affecter les trois piliers de la sécurité des actifs informationnels que sont la disponibilité, l'intégrité et la confidentialité.

3.9 Rédaction d'une politique de gestion du filtrage Web

La gestion du système de filtrage Web de l'Agence nécessite l'établissement d'une politique afin d'encadrer la gestion de celui-ci. Par exemple, on doit établir quel est le processus afin d'autoriser l'accès à des sites Internet (Facebook, Hotmail ou des sites plus sensibles) à l'ensemble du personnel ou quelques personnes seulement. De plus, le mécanisme d'enquête sur l'utilisation d'Internet par le personnel de l'Agence doit être bien encadré. Avec la collaboration de l'Agence de la santé et des services sociaux de la Capitale Nationale (qui a partagé leur politique de filtrage), nous avons un bon point de départ pour l'établissement de notre politique.

3.10 Rencontre avec l'auditeur externe

L'auditeur externe mandaté par l'Agence pour réaliser l'audit des états financiers, a réalisé dans le cadre de son audit, certains travaux relatifs à la sécurité des systèmes financiers. Le RSAI effectuera un suivi sur la mise en place des différentes recommandations proposées par l'auditeur externe.

3.11 Préparation du bilan de sécurité selon le gabarit produit par le Ministère de la Santé et des services sociaux du Québec (MSSS)

Le 5 mars 2014, Monsieur Richard Audet, sous-ministre associé à la direction générale des technologies du MSSS faisait parvenir aux PDG des agences de santé et de services sociaux du Québec un courriel contenant un gabarit portant sur la sécurité des actifs informationnels. Le bilan a été complété par le RSAI et envoyé à la coordonatrice régionale de la sécurité des actifs informationnels (CRSAI) de la région de Montréal. Les différents bilans des établissements de la région montréalaise devaient être compilés et les résultats envoyés au MSSS pour le 1er juin 2014.

3.12 Directive concernant le cadre de gestion de la sécurité de l'information produit par le Ministère de la Santé et des services sociaux du Québec (MSSS)

Le 6 mars 2014, Monsieur Richard Audet, sous-ministre associé à la direction générale des technologies du MSSS faisait parvenir aux PDG des agences de santé et de services sociaux du Québec un courriel concernant l'approbation par le Secrétariat du Conseil du trésor d'une nouvelle directive sur la sécurité de l'information.

La vision gouvernementale en sécurité de l'information prévoit :

- Une approche stratégique triennale en sécurité de l'information pour 2014-2017 (C.T. 213483) ;
- Un cadre gouvernemental de gestion de la sécurité (C.T. 213482) ;
- Un cadre de gestion des risques et des incidents (C.T. 213484).

Cette nouvelle directive fût présenté au membres du comité de sécurité des actifs informationnels qui s'est tenu au mois de juin 2014.

3.13 Essai d'un programme de sensibilisation à la sécurité de l'information offert par le centre de service partagés du Québec (CSPQ)

Le RSAI a fait l'essai d'un programme de sensibilisation à la sécurité de l'information (version démo). De nombreux sujets sont abordés tel que :

- Principe du bureau propre ;
- Utilisation des mots de passe de façon sécuritaire ;
- Ingénierie sociale.

3.14 Réalisation d'une première analyse de vulnérabilités (Site St-Denis et Pavillon Lafontaine)

Le RSAI a effectuée une première analyse de vulnérabilités sur les équipements informatiques (serveurs) utilisés par le personnel du site St-Denis ainsi que du Pavillon Lafontaine. Les deux analyses ont révélées certaines vulnérabilités pour lesquels un rapport a été produit avec des mesures à mettre en place pour atténuer les risques.

3.15 Réalisation d'une première analyse de vulnérabilités (Technocentre)

Le RSAI a effectuée une première analyse de vulnérabilités sur certains équipements informatiques (serveurs) utilisés au Technocentre régional de Montréal. L'analyse a mis en lumière certaines vulnérabilités pour lesquels un rapport a été produit avec des mesures à mettre en place pour atténuer les risques.

3.16 Conseils sur différents projets technologiques de l'Agence

Le RSAI est amené à conseiller les différentes équipes de l'Agence sur les aspects touchant la sécurité des actifs informationnels au niveau des projets technologiques qui doivent être réalisées. Ci-dessous une liste non exhaustive concernant l'implication du RSAI au niveau des différents projets mise en place par l'Agence.

- Système informatique des guichets d'accès aux services spécialisés, services diagnostiques et programmes-services (SIGASS) ;
- Accès Internet au serveur de rapports (SSRS) ;
- Solution régionale de laboratoire (SRL) ;

3.17 Intérim à coordination régionale de la sécurité des actifs informationnels pour la région de Montréal (CRSAI)

Le RSAI assure depuis le mois de juillet 2014, l'intérim comme CRSAI. La personne occupant le poste actuellement étant en prêt de service au Ministère de la santé et des services sociaux du Québec (MSSS). Avec la mise en place du PL-10, le poste n'a pas été comblé par une autre personne. La liste ci-dessous n'est pas exhaustive concernant les tâches effectuées par le CRSAI

- Analyser les demandes de dérogation aux différentes politiques du MSSS ;
- Collaborer avec le MSSS sur la mise en place de nouvelles règles de sécurité ;
- Conseiller les établissements au niveau de la sécurité des actifs informationnels ;
- Intervenir auprès des établissements lorsque survient des virus informatiques ;
- Transmettre aux établissements les avis et directives provenant du MSSS.

3.18 Sensibilisation du personnel de l'Agence

Le RSAI rencontre tous les employés nouvellement embauchés par l'Agence sur ses différents sites (siège social, Technocentre et Pavillon Lafontaine) afin de les sensibiliser à la sécurité des actifs informationnels. Il y a eu près de 120 personnes qui ont été rencontrées par le RSAI durant la période 2013-2015.

La sensibilisation est l'un des points les plus importants. Celle-ci doit se faire de façon continue. Pour ce faire, la sensibilisation peut se fait de plusieurs façons :

- Rencontre des employés nouvellement embauchés ;
- Rencontre des employés œuvrant en technologies de l'information ;
- Rencontre des gestionnaires leur expliquant leur rôle en lien avec la sécurité des actifs informationnels ;
- Publication de messages sur l'intranet de l'Agence.

3.19 Rencontres du Comité de sécurité des actifs informationnels (CSAI)

Le Comité de sécurité des actifs informationnels est un comité permanent qui a été créé en mai 2006. Il est composé de représentants de toutes les directions de l'Agence et il se réunit trois fois par année. Celui-ci s'est réuni six fois pendant la période 2013-2015. Le comité peut également se réunir si une situation particulière l'exigeait. Celui-ci assure un rôle de soutien et de conseil auprès du RSAI. Également, le comité participe aux orientations en ce qui a trait à l'application des mesures touchant le Cadre global de gestion des actifs informationnels.

Voici les principaux dossiers discutés lors des rencontres du comité :

- Analyse de vulnérabilités ;
- Directive gouvernementale en matière de sécurité de l'information ;
- Politique de mots de passe ;

- Plan de relève ;
- Sensibilisation à la sécurité des actifs informationnels.

La composition des membres ainsi que les différents mandats du comité de la sécurité des actifs informationnels (CSAI) se retrouve à l'annexe 4.

5. PLAN D'ACTION 2015-2016

Suite aux différentes observations soulevées par l'auditeur externe, par certaines faiblesses notées par l'audit interne concernant les 15 mesures obligatoires du Cadre global, par les commentaires du RSAI, par les demandes incluses dans l'entente de gestion et d'imputabilité 2013-2014 entre l'Agence de Montréal et le ministère de la Santé et des Services sociaux du Québec, par le bilan de sécurité de l'information envoyé au MSSS et dans un souci d'amélioration continue, voici les actions de sécurité proposées pour la prochaine année.

La nature des actifs (données nominatives et cliniques) nécessite la mise en place des recommandations afin de réduire les risques appréhendés.

Tout d'abord, il faut poursuivre la mise en place des mesures proposées dans le plan d'action 2013-2014. Il y a des recommandations qui sont partiellement complétée et nous devons poursuivre la mise en place de celles-ci.

R.1 Effectuer des tests mensuels de recouvrement du système (copies de sécurité)

Action
Mettre en place un processus qui permet d'effectuer des tests de recouvrement avec les copies de sécurité.

R.2 Mettre en place un plan de continuation des affaires ainsi qu'un plan de relève informatique au Technocentre régional de Montréal

Action
Débuter le processus d'analyse afin d'évaluer la mise en place de ce type de plan.

R.3 Surveiller les équipements (applications, matériels et logiciels) avec un logiciel de type corrélateur d'événement

Action
Effectuer la mise en place d'un logiciel permettant la corrélation d'événement (« Security information and event management »).

R.4 Mettre un processus formel de gestion des risques

Action
Débuter l'analyse d'impact sur la mise en place du processus de gestion des risques. Cette recommandation provient de la gestion organisationnelle de la sécurité de l'information proposée par le MSSS.

R.5 Effectuer régulièrement des tests de données

Action
Effectuer un test de recouvrement des données financières avec les copies de sécurité.

R.6 Mettre en place des coupe-feux (confidentialité)

Action

Poursuivre la réalisation de ce dossier niveau du CIUSSS Centre-Est-de-l'Île-de-Montréal.

6. CONCLUSION

La sensibilisation des différents acteurs (haute direction, cadre, personnel en technologie de l'information et les utilisateurs) demeure une activité importante qu'il faut maintenir. Avec la collaboration et l'implication de tout le monde, les facteurs de réussite au niveau de la sécurité des actifs informationnels ne sont qu'améliorés.

Avec l'adoption du projet de loi n°10, la mise en place des recommandations prévues dans le présent document se poursuivra au niveau du CIUSSS Centre-Est-de-l'Île-de-Montréal.

La sécurité des actifs informationnels est un domaine en constant changement avec l'avènement de nouvelles technologies. Les nouvelles façons de faire que peuvent utiliser des personnes mal intentionnées sont nombreuses et demandent une vigilance accrue. Selon des études, les renseignements de santé sont de plus en plus recherchés par des personnes ou organisations malveillantes pour la valeur que ceux-ci ont sur le marché noir (pour le vol d'identité par exemple). C'est pour cette raison qu'il faut poursuivre une vigie en sécurité de l'information afin d'être au courant des nouveaux types d'attaques et de vulnérabilités pouvant être utilisés contre les actifs informationnels.

La sécurité des actifs informationnels est un travail de tous les jours, car personne ne peut être à l'abri à 100 % des risques pouvant affecter les actifs. Notre travail est de mettre en place les mesures qui permettent de mitiger les risques touchant les actifs informationnels de l'Agence.

Nous devons maintenir une vigilance accrue afin de protéger le plus efficacement possible les actifs informationnels.

7. LISTE DES ANNEXES

Annexe 1 : Rôles des intervenants/entités à l'Agence dans la protection des actifs informationnels

Annexe 2 : 15 mesures prioritaires du Cadre global

Annexe 3 : Recommandations suite à l'audit interne croisé réalisé sur les sites de l'Agence

Annexe 4 : Composition et mandats du comité de sécurité des actifs informationnels (CSAI)

Annexe 1 – Rôles des intervenants/entités à l'Agence dans la protection des actifs informationnels

La sécurité des actifs informationnels comporte plusieurs enjeux – qu'ils soient d'ordre organisationnel, professionnel, économique, technologique, politique, éthique ou légal – et les mesures visant à assurer cette sécurité intéressent plus que jamais aussi bien les hautes instances gouvernementales que les gestionnaires, les spécialistes et le personnel du système de santé ainsi que toute personne ayant accès aux renseignements personnels et aux autres informations numériques. La gestion de la sécurité des actifs informationnels devient une préoccupation partagée par tous les acteurs concernés par cette question. Le tableau ci-dessous précise les responsabilités des différents intervenants impliqués dans la chaîne de la sécurité des actifs informationnels.

Intervenant/entité	Rôles/Responsabilités
Conseil d'administration (C.A)	• Approuver la politique de sécurité des actifs informationnels de l'Agence ; • Adopter le bilan annuel de sécurité des actifs informationnels
Présidente-directrice générale (PDG)	• Nommer le responsable de la sécurité des actifs informationnels (RSAI). Cette nomination doit être entérinée par le conseil d'administration; • Voir à ce que les valeurs et les orientations en matière de sécurité soient partagées par l'ensemble des gestionnaires et du personnel; • S'assurer de sa mise en œuvre et du suivi de son application; • Soumettre le bilan annuel résultant de l'application de la Politique au conseil d'administration; • Apporter les appuis financiers et logistiques nécessaires à la mise en œuvre de la politique de sécurité des actifs informationnels.
Comité de la sécurité des actifs informationnels (CSAI)	• Conseiller le RSAI; • Assurer l'application des différentes mesures de sécurité identifiées dans le CGGAI–volet sécurité, soutien la mise en place des dispositions législatives et proposer des mesures communes pour assurer la disponibilité, l'intégrité, la confidentialité de l'information ainsi que l'authentification et l'irrévocabilité de l'usager s'appliquant à l'ensemble des actifs informationnels de l'Agence; • Évaluer les incidences sur la sécurité de l'organisation que les nouveaux projets pourraient avoir; • Constituer 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 regard de l'élaboration, de la mise en œuvre et de la mise à jour des mesures prévues au plan directeur de sécurité de l'information de l'Agence; • Effectuer le suivi de l'échéancier et rendre des comptes au PDG.
Responsable de sécurité des actifs informationnels (RSAI)	• Élaborer la politique sur la sécurité des actifs informationnels qui sera adoptée par l'organisme et soumettre cette politique au

Intervenant/entité	Rôles/Responsabilités
	directeur général et au conseil d'administration de l'Agence pour approbation; • Mettre en place et présider le CSAI, qui est formé du responsable de la sécurité, de gestionnaires, d'un vérificateur interne, de détenteurs, de représentants des ressources humaines, financières et matérielles ainsi que d'un juriste; • Coordonner, avec les secteurs visés et en concordance avec les orientations régionales, la mise en œuvre de la politique sur la sécurité des actifs informations adoptée par l'Agence et en suivre l'évolution; • Identifier, en collaboration avec les gestionnaires, les détenteurs d'actifs informationnels dans leur secteur respectif; • S'informer des besoins en matière de sécurité auprès des détenteurs et des gestionnaires, leur proposer des solutions et coordonner la mise en place de ces solutions; • Gérer les aspects relatifs à l'escalade des incidents de sécurité de l'information ; • Suivre la mise en œuvre de toute recommandation découlant d'une vérification ou d'un audit ; • Produire annuellement, et au besoin, les bilans et les rapports relatifs à la sécurité des actifs informationnels appartenant à l'établissement en s'assurant que l'information sensible à diffusion restreinte est traitée de manière confidentielle et, après approbation de la PDG et du conseil d'administration, les soumettre au coordonnateur régional de la sécurité des actifs informationnels.
Direction des technologies et systèmes d'information (DTSI)	• Fournir et maintenir en état les moyens techniques de sécurité dans l'exploitation des actifs informationnels; • Assurer la conformité de ces moyens techniques en fonction des besoins de sécurité déterminés par le détenteur d'actif; • Assister et conseiller les utilisateurs en vue d'une meilleure utilisation de ces moyens techniques; • Mettre en application la Politique de compte d'usagers, les procédures des profils et des codes d'accès; • Voir à la tenue des inventaires sur les équipements et logiciels; • Voir à la gestion des mots de passe; • Voir à la mise en place des antivirus et à la tenue des journaux; • Assurer la sécurité dans le développement d'applications informatiques; • Mettre en place et maintenir une relève des actifs informationnels classés prioritaires; • Conseiller les gestionnaires de l'Agence dans l'acquisition des équipements, des logiciels et du matériel nécessaires pour appliquer la Politique de sécurité des actifs informationnels de l'Agence;

Intervenant/entité	Rôles/Responsabilités
	• Voir à la mise en place des mesures de sécurité physique pour les contrôles d'accès aux salles des serveurs, aux équipements de télécommunication ou à tout autre matériel informatique; • Appuyer le RSAI dans son rôle.
Gestionnaires et détenteurs des actifs	• Autoriser les droits d'accès aux informations dont ils sont détenteurs; • Évaluer les risques et déterminer le niveau de protection visé; • Élaborer les contrôles non informatiques (par exemple la séparation des tâches); • Voir au suivi des codes de conduite émis par le Service des ressources humaines; • S'assurer que son personnel est au fait de ses obligations découlant de la Politique de sécurité des actifs informationnels de l'Agence, normes et procédures de sécurité en vigueur.
Direction des affaires institutionnelles et des ressources humaines (DAIRH)	• Informer tout nouveau membre du personnel de ses obligations découlant de la Politique de sécurité des actifs informationnels de l'Agence; • Sensibiliser tout nouveau membre du personnel aux enjeux reliés à la sécurité des actifs informationnels**;** • S'assurer de la signature de l'engagement au secret professionnel et à la confidentialité des données par tout nouveau membre du personnel.
Utilisateurs	• Prendre connaissance de la Politique de sécurité; • Respecter la Politique de sécurité des actifs informationnels de l'Agence, normes, directives et procédures en vigueur en matière de sécurité de l'information et les autres politiques et directives en découlant ; • Signer le formulaire d'engagement au secret professionnel et à la confidentialité des données, et les autres formulaires(s) d'engagement selon le(s) service(s) utilisé(s); • Aviser le supérieur hiérarchique dès qu'il constate un manquement à la Politique.

Annexe 2 -15 mesures prioritaires du Cadre global

Ces mesures et directives de sécurité sont des énoncés permettant d'indiquer quels sont les standards de l'Agence en matière de sécurité. Elles indiquent les règles à suivre afin de se conformer aux énoncés de la politique de sécurité. Issues du Cadre global, ces 15 mesures prioritaires ont été implantées dans les 4 installations de l'Agence depuis octobre 2008. Des vérifications périodiques sont effectuées pour s'assurer de leur conformité ;

Mesures	Résultats
1. Sensibilisation et formation du personnel sur la politique de sécurité	La sensibilisation se fait de façon continue auprès du personnel en utilisant diverses plateformes : • Utilisation de l'intranet local et régional de l'Agence • Rencontres des nouveaux employés avec le responsable de la sécurité des actifs pendant le premier mois d'emploi • Utilisation d'une bannière lors de l'ouverture d'une session de travail • Intégration d'un message de confidentialité dans les courriers électroniques
2. Gestion des antivirus	Tous les postes et serveurs sont munis d'un logiciel antivirus pour la protection contre les logiciels malicieux.
3. Utilisation d'un site de conservation externe	Mécanisme de protection des données critiques, pour la récupération des données en cas de perte. Le site de la Direction de santé publique et l'Agence (3725, rue St-Denis) utilisent un fournisseur externe pour l'entreposage des rubans de sauvegarde tandis que le Technocentre utilise ses 2 sites en complément l'un de l'autre.
4. Application d'un plan de sauvegarde et de récupération	Une stratégie de sauvegarde et de récupération de données est mise en place afin d'en assurer l'intégrité et la disponibilité. Ce plan précise la fréquence de sauvegarde des copies, le lieu d'entreposage et les personnes responsables.
5. Gestion des licences et inventaires de matériels et logiciels	Processus de gestion qui permet avec un logiciel et des bases de données de faire l'inventaire en temps réel. Ceci afin de constituer et tenir à jour les équipements, les logiciels et les applications.
6. Mise en place d'un processus d'escalade	Le processus d'escalade est une mesure exceptionnelle qui permet de contacter des personnes clés et de poser des gestes appropriés lorsque des d'incidents critiques surviennent. Les rôles et responsabilités sont assignés aux personnes impliquées dans la gestion de ces incidents selon une gradation.
7. Utilisation d'un logiciel pour améliorer la sécurité du support à distance	Un logiciel certifié par le MSSS est utilisé pour le support à distance afin d'assurer la confidentialité des données et l'imputabilité du personnel informatique pendant l'accès.
8. Mise en place de moyens permettant la sécurité physique pour l'emplacement des installations (matériel informatique /télécommunications)	Des mécanismes de sécurité sont en place pour assurer la sécurité des lieux. Par exemple, la DSP et le Technocentre ont des caméras pour visualiser les faits et gestes des intervenants.

Mesures	Résultats
9. Utilisation de coffres de rangement à l'épreuve du feu, homologués, avec boîtier pour média informatique	Des voûtes et des coffres à l'épreuve du feu sont disponibles pour protéger les originaux des logiciels et les documents importants et/ou critiques.
10. Existence de moyens conformes pour l'extinction des incendies	Pour la prévention contre le feu, les sites du Technocentre et Saint-Denis sont conformes en ayant des détecteurs de fumée, des gicleurs et un système relié à une centrale. La salle de la DSP n'est pas conforme au modèle proposé.
11. Contrôle d'accès général et aux salles de serveurs	Des cartes d'accès et des registres sont en place afin de limiter les accès non autorisés.
12. Mise en place de moyens permettant une alimentation électrique sans interruption	Toutes les salles ont une alimentation électrique sans interruption avec des batteries pour prendre la relève du circuit électrique en cas de perturbations ou de panne générale.
13. Politique de contrôle de la sécurité logique	Un mécanisme d'identifiant et d'autorisation est mis en place pour limiter les accès aux seules personnes autorisées. L'accès à l'information est contrôlé par un identifiant unique pour chaque utilisateur du réseau informatique. En collaboration avec les gestionnaires, une stratégie de groupe est déterminée selon les besoins spécifiques.
14. Politique des comptes usager	Une politique de gestion des comptes usager et des mots de passe est en place et un journal d'accès est maintenu pour assurer l'imputabilité.
15. Maintenance des comptes usagers	Un outil de gestion des codes d'usagers, des profils et de leurs répertoires d'usagers, conçu pour permettre l'extraction de plusieurs listes pour la gestion des accès au réseau. Ceci permettra de gérer efficacement la désactivation ou la suppression des codes d'usagers inutilisés après une certaine période.

Annexe 3 – Recommandations suite à l'audit interne croisé des 16 et 17 octobre 2013

Agence (3725, St-Denis)

1.2. Mettre en place pour le personnel des technologies de l'information
- des rencontres sur différents sujets touchant la sécurité des actifs informationnels.
- un document de présentation.
- une capsule sur intranet ou un courriel.

4.3. Effectuer des tests mensuels de recouvrements du système.

8.1. Retirer ces éléments de la salle, ou déplacer la poubelle à l'extérieur à chaque fin de session.

11.1. Remplacer le registre papier par un système à carte magnétique pour plus d'imputabilité.

11.2. Réviser annuellement la liste d'accès à la salle informatique.
- Installer une caméra de surveillance ou un lecteur de carte magnétique.

Technocentre

1.2. Mettre en place pour le personnel des technologies de l'information
- des rencontres sur différents sujets touchant la sécurité des actifs informationnels.
- un document de présentation.
- une capsule sur intranet ou un courriel.

3.1. Sécuriser les sauvegardes sur site externe

4.3. Effectuer des tests mensuels de recouvrements du système.

5.2. Effectuer une vérification bisannuelle de l'inventaire des logiciels installés.

Pavillon Lafontaine

1.2. Mettre en place pour le personnel des technologies de l'information
- des rencontres sur différents sujets touchant la sécurité des actifs informationnels.
- un document de présentation.
- une capsule sur intranet ou un courriel.

8.2. et 10.1. Installer des gicleurs dans la salle des serveurs.

11.1. Remplacer le registre papier par un système à carte magnétique pour plus d'imputabilité.

Annexe 4 – Composition et mandats du comité de sécurité des actifs informationnels (CSAI)

Composition du comité en date du 3 mars 2014 :

- Mme Liette Pigeon, spécialiste en procédés administratifs, Direction des affaires cliniques, médicales et universitaires;
- M. Christian Bertrand, coordonnateur, Direction des technologies et systèmes d'information;
- Mme Loraine Desjardins, adjointe à direction générale, Direction générale;
- Mme Caroline Dusablon, agente de planification, Direction des affaires institutionnelles et des ressources humaines;
- M. Denis Hébert, chef de service, Direction des affaires institutionnelles et des ressources humaines;
- M. Stéphane Gagnon, responsable de la sécurité des actifs informationnels, Direction générale;
- Mme Hélène Gendron, chef de service, Direction des technologies et systèmes d'information;
- Mme Liette Bernier, directrice adjointe, Direction des programmes-services;
- Mme Céline Roy, commissaire régionale aux plaintes et à la qualité des services;
- M. Serge Laniel, coordonateur, Direction des technologies et systèmes d'information;
- M. Roger Martin, conseiller-cadre, Direction des immobilisations, technologies médicales et approvisionnements régionales.

Mandat :

- Conseiller le responsable de la sécurité des actifs informationnels (RSAI);
- Proposer des orientations et faire des recommandations dans l'élaboration, la mise en œuvre et la mise à jour des mesures prévues au plan de directeur de sécurité de l'information;
- Évaluer les incidences sur la sécurité des actifs informationnels de l'Agence que les nouveaux projets pourraient avoir;
- Vérifier et recommander l'application des différentes mesures de sécurité identifiées dans le Cadre global et soutenir la mise en place des dispositions pour assurer la disponibilité, l'intégrité, la confidentialité de l'information ainsi que l'authentification et l'irrévocabilité des actions s'appliquant à l'ensemble des actifs informationnels;
- Élaborer et s'assurer de la mise à jour de la politique de sécurité des actifs informationnels ;
- S'assurer de la mise en application des mesures de sécurité des actifs informationnels ;
- Commenter les différents documents déposés au comité ;
- Effectuer la révision des rapports sur les risques et menaces des actifs informationnels ;
- Effectuer la révision des rapports d'incidents des actifs informationnels ;
- Proposer et décider des activités de vérification pertinentes dans l'utilisation des actifs informationnels ;

- Recommander la mise en place des programmes de prévention pour assurer la sécurité des actifs informationnels ;
- Analyser les circonstances reliées aux mesures disciplinaires et recommander que des sanctions soient imposées lors d'incidents touchant les actifs informationnels ;
- Proposer et approuver un plan de sensibilisation/formation à l'ensemble du personnel.