Bilan de la sécurité des actifs informationnels

2011-2013

Agence de la santé et des services sociaux de Montréal

Québec

Bilan de la sécurité des actifs informationnels 2011-2013

Agence de la santé et des services sociaux de Montréal

Juillet 2013

Approuvé par le conseil d'administration du 24 septembre 2013

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 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
Juillet 2013

Bilan de la sécurité des actifs informationnels 2011-2013

ISBN 978-2-89510-627-2 (version imprimée)
ISBN 978-2-89510-628-9 (PDF)

Dépôt légal - Bibliothèque et Archives nationales du Québec, 2013

Ce document est disponible :
au centre de documentation de l'Agence : 514 286-5604
à la section «Publications de l'Agence» du site Internet : http://agence.santemontreal.qc.ca/

TABLE DES MATIÈRES

PRÉAMBULE

Le présent bilan sur la sécurité des actifs informationnels de l'Agence de la santé et des services sociaux de Montréal est présenté pour une seconde année au conseil d'administration et couvre la période 2011-2013. Ce bilan respecte ainsi une recommandation émise en 2011 par l'auditeur externe qui demandait qu'un bilan soit déposé annuellement au conseil d'administration de l'Agence. 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 2011-2013 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 cinq 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* ».

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 (3725, rue St-Denis), siège social
2- La Direction de santé publique (1301, rue Sherbrooke Est, pour la vigie et la surveillance en santé publique)
3- Le Technocentre régional (400, boul. de Maisonneuve-Ouest, pour l'hébergement, la gestion des systèmes et applications des établissements de la région et du Dossier de santé du Québec (DSQ)
4- Le Technocentre régional (4835, avenue Christophe-Colomb, pour la relève OACIS et le système d'imagerie)

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

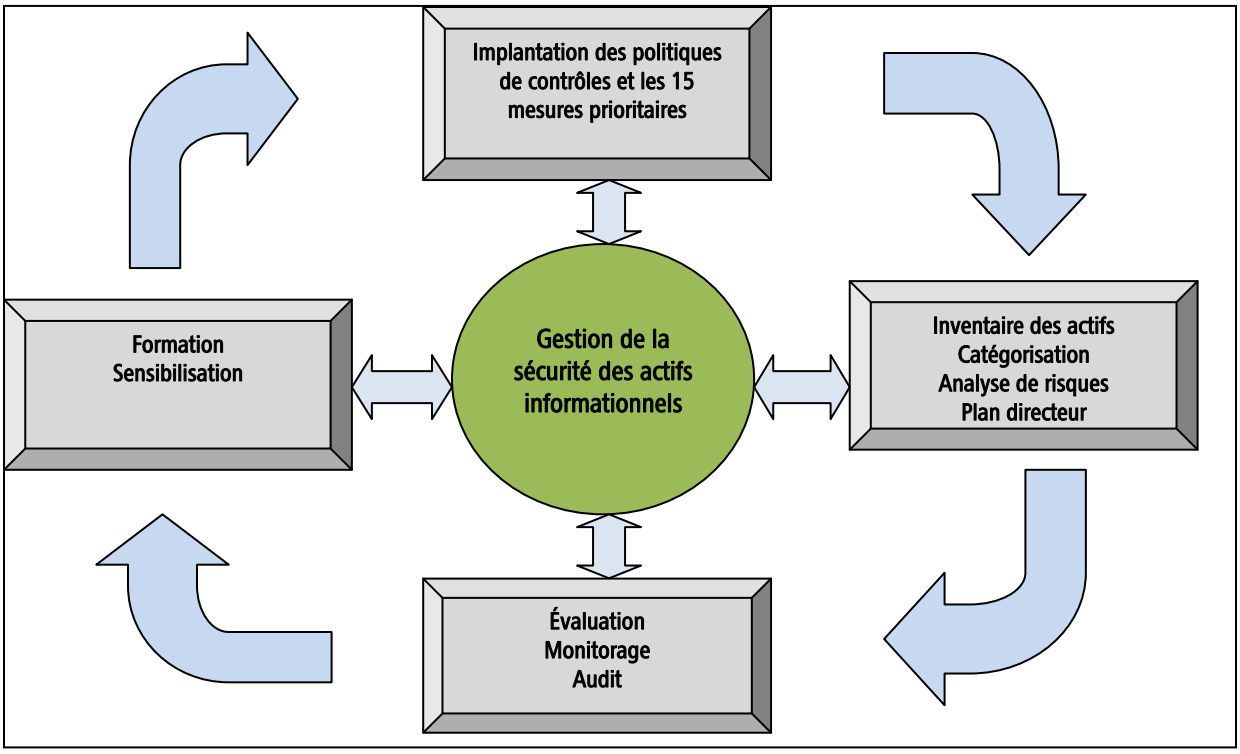

Fig. 1 Gestion de la sécurité des actifs informationnels

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 du financement, de la performance et des technologies de l'information
Gestionnaires et détenteurs des actifs
Direction du secrétariat général, de l'administration, des ressources humaines et des communications
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. Bilan annuel des activités et des réalisations

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. Nous nous attarderons principalement sur les faits saillants de la dernière année.

Année	Réalisations
Février 2012	Nomination d'un nouveau RSAI
Avril 2012	Réalisation d'un audit interne sur l'implantation des 15 mesures prioritaires du Cadre global
Juin 2012	Élaboration d'une politique des accès logiques aux fournisseurs
Juillet 2012	Mise à jour de la politique de sécurité des actifs informationnels
Octobre 2012	Analyse de sécurité sur l'utilisation du produit « valise de garde »
Octobre 2012	Mise à jour de la gestion des risques majeurs à l'Agence
Octobre 2012	Participation à la mise en place d'une autorité de certification au Technocentre
Novembre 2012	Participation à la mise en place du filtrage Web pour la région de Montréal
Novembre 2012	Collaboration à la rédaction de la politique d'utilisation des médias sociaux
Novembre 2012	Réalisation d'un test d'intrusion au Technocentre de Montréal
Mars 2013	Participation à la certification par le CRIM de l'application Jérôme Plus pour la banque d'interprètes
Mars 2013	Rencontre avec l'auditeur externe
Septembre 2013	Dépôt du bilan annuel de la sécurité des actifs informationnels 2012

3.1. 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 avril 2012, un second 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 et représentante sécurité, Pavillon Lafontaine), M. André Côté (analyste informatique, Saint-Denis) et M. Martin Villeneuve (analyste informatique et représentant sécurité, 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.

3.2. Élaboration d'une politique des accès logiques aux fournisseurs

L'Agence désire se doter d'une politique de gestion des accès aux fournisseurs. Le but de cette politique est d'harmoniser la gestion des accès aux différents fournisseurs qui accèdent aux différents actifs informationnels de l'Agence. Le Technocentre régional de Montréal transige avec plus de quarante fournisseurs. Étant donné la complexité des différents systèmes utilisés au Technocentre, il faut s'assurer que la mise en place d'une telle politique sécurise les actifs informationnels tout en demeurant fonctionnelle lorsqu'une intervention est nécessaire. Cette politique est en cours de rédaction et sera présentée au CSAI de l'Agence pour approbation. Par la suite, elle sera mise en application sur tous les sites de l'Agence.

3.3. Mise à jour et adoption de la politique de sécurité des actifs informationnels

Une nouvelle version de la politique de sécurité de l'Agence est en cours de rédaction et sera déposée pour adoption au conseil d'administration au cours de l'année 2013. La mise à jour de la politique se concentre principalement sur la gestion des renseignements personnels.

Cette politique constitue la pierre angulaire et le fondement du programme de sécurité des actifs informationnels de l'Agence. Elle indique les attentes et les objectifs de l'Agence en matière de sécurité ainsi que les moyens à prendre pour les atteindre. Elle sert de plus, à structurer et coordonner les efforts de sécurité et à assurer le respect de toute législation à l'égard de l'usage et du traitement de l'information (électronique et papier), de l'utilisation des technologies de l'information et des télécommunications, ou autres manipulations de l'information.

La portée de la politique de sécurité s'applique à toute personne physique ou morale qui utilise ou accède à de l'information, quelque soit le support sur lequel elle est manipulée, en transit ou conservée. Des normes, guides et procédures viennent l'appuyer afin de préciser les obligations qui en découlent.

3.4. Analyse de sécurité sur l'utilisation du produit « valise de garde »

Le produit « valise de garde » est un service hébergé chez un fournisseur externe. Celui-ci serait utilisé par l'équipe des mesures d'urgence de l'Agence.

Le projet « Valise » de garde permet :

- d'avoir une liste d'appel qui demande une confirmation de réception du message
- d'utiliser des services de géomatique (pour localiser les centres hospitaliers par exemple)

Le RSAI a produit une grille d'évaluation permettant d'évaluer les aspects touchant la sécurité des actifs informationnels (sécurité physique, logique, chiffrement des données, sensibilisation du personnel).

3.5. Mise à jour des risques majeurs touchant l'Agence

En octobre 2010, 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.

En 2012, le MSSS demandait aux agences une mise à jour de cette analyse.

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 de relève du réseau de télécommunications particulièrement 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.
Pérennité des actifs technologiques	Remplacement de l'outil de contrôle d'accès et de filtrage Internet à la DSP. Consolidation et transfert d'équipements entre le siège social et le Technocentre. Consolidation et transfert d'équipements entre la Direction de santé publique et le Technocentre.
Intrusion à son réseau informationnel	Consolidation des journaux de sécurité par le déploiement d'un outil de journalisation au Technocentre. Réalisation d'un test d'intrusion au Technocentre.
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 de relève du réseau de télécommunications au Technocentre	Mise en place d'une infrastructure de relève pour les applications critiques.

3.6. Participation à la mise en place d'une autorité de certification au Technocentre

En collaboration avec les équipes du Technocentre, nous travaillons à mettre en place une autorité de certification.

Selon l'Office québécois de la langue française, une autorité de certification se définit comme un : « Organisme reconnu dont le rôle est de délivrer et de gérer des certificats numériques ».

Une autorité de certification permet de valider l'identité du demandeur, celui-ci peut être un utilisateur ou un équipement informatique. Par la suite, l'utilisation du chiffrement est possible, c'est-à-dire de chiffrer (rendre illisible) les communications. Pour déchiffrer (rendre lisible) les communications, il faut détenir la clé qui a effectué le chiffrement. Les principaux avantages sont d'assurer l'intégrité (que les données n'ont pas été modifiées) et qu'elles proviennent bien de l'expéditeur.

3.7. 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.

3.8. Collaboration à la rédaction de la politique d'utilisation des médias sociaux

Le RSAI collabore actuellement avec la Coordination des communications à une mise à jour de la politique d'utilisation des médias sociaux à l'Agence. Ce dossier est d'actualité avec la prolifération des différentes plateformes de médias sociaux. Il est important de sensibiliser les utilisateurs sur les comportements acceptables et non acceptables lors de l'utilisation des médias sociaux.

3.9. Réalisation d'un test d'intrusion au Technocentre de Montréal

En novembre 2012, l'Agence a mandaté un fournisseur externe afin d'effectuer un test d'intrusion aux actifs informationnels situés au Technocentre régional de Montréal. Tout d'abord, le fournisseur a tenté de s'introduire à partir de l'extérieur du réseau de la santé et des services sociaux en utilisant un actif informationnel appartenant à l'Agence de Montréal. Par la suite, le test s'est poursuivi à l'interne, c'est-à-dire que le fournisseur était directement relié au réseau informatique du Technocentre régional de Montréal. Les résultats du test d'intrusion ont démontré des forces ainsi que certaines lacunes pour lesquelles un plan d'action propose les mesures nécessaires afin de réduire les risques identifiés.

3.10. Participation à la certification par le CRIM de l'application Jérôme Plus pour la banque d'interprètes

L'application Jérôme Plus est un système d'information de gestion des demandes de service d'interprétation. Par exemple, un professionnel de la santé ne maîtrisant pas la langue étrangère de l'usager (patient) requiert la présence d'un interprète. Le RSAI a participé avec les différentes équipes impliquées dans le projet sur les différents aspects touchant les mesures de sécurité à mettre en place afin que l'application obtienne la certification délivrée par le ministère de la Santé et des Services sociaux.

3.11. 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.

3.12. Dépôt du bilan annuel de la sécurité des actifs informationnels

La production du présent document fait suite à une recommandation de l'auditeur externe concernant la production d'un bilan annuel sur la sécurité des actifs informationnels. Le précédent bilan couvrait une période de six ans. De plus, 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, il est mentionné de produire un bilan portant sur les actions réalisées en sécurité de l'information.

3.13. 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.

Avec l'interprétation des résultats du sondage réalisé en 2011 portant sur la sécurité des actifs informationnels, 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.
- Matériel promotionnel.

3.14. 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 quatre fois par année. 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 :

- Filtrage Web.
- Risques associés à l'utilisation de produits permettant le partage de documents.
- Sensibilisation à la sécurité des actifs informationnels.
- Test d'intrusion.
- Test de relève.

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

4. Recommandations

4.1. Cinq sources

Les recommandations qui suivent proviennent des cinq sources internes et externes qui ont généré 22 recommandations pour lesquels un plan d'action est énoncé à la section 5 du présent document.

L'ensemble de ces recommandations vise l'atteinte d'un seul et même objectif, celui de réduire les risques pouvant affecter les actifs informationnels.

4.1.1. Audit interne

15 mesures prioritaires du cadre global : 6 recommandations

Il sert à s'assurer que les 15 mesures prioritaires sont bien implantées sur l'ensemble des installations de l'Agence. Plusieurs recommandations ont été énoncées (voir l'annexe 3 du présent document) et ont déjà été mises en place afin de palier aux lacunes :

- Installer le logiciel antivirus (plateforme Macintosh et serveur de développement informatique du siège social)
- Augmenter la longueur des mots de passe à 8 caractères et complexifier sa composition (Pavillon Lafontaine)
- Sécuriser le transport des copies de sécurité entre le siège social et le Technocentre

Il y a plusieurs mesures obligatoires qui n'ont pas fait l'objet de recommandations car celles-ci étant déjà en place sur l'ensemble des sites de l'Agence.

Une cote (C) Conforme, (NC) Non-Conforme ou (NCA) Non-Conforme Acceptable était attribué selon les réponses obtenues lors de la réalisation de l'audit. Plusieurs éléments ayant été corrigés en cours d'année ne se retrouve pas dans le présent bilan.

Voici les recommandations concernant l'audit interne :

R.1.	Identifier le log du système d'exploitation permettant d'identifier les accès et les tentatives infructueuses (Pavillon Lafontaine)
R.2.	Mettre en place un programme de sensibilisation à la sécurité des actifs informationnels pour le personnel des technologies de l'information
R.3.	Prévoir un mécanisme de protection pour les ordinateurs portatifs ainsi que les appareils mobiles
R.4.	Remplacer le registre papier par un système à carte magnétique pour plus d'imputabilité (Siège social et Pavillon Lafontaine)
R.5.	Effectuer une vérification bisannuelle de l'inventaire des logiciels installés
R.6.	Installer des gicleurs dans la salle des serveurs (Pavillon Lafontaine)

4.1.2. 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 : 2 recommandations

L'entente de gestion et d'imputabilité (EGI), selon la Loi sur la santé et les services sociaux (LSSS), est un contrat annuel qui lie le MSSS et l'Agence au sujet des objectifs que celle-ci doit atteindre.

L'entente mentionne que l'on doit : « Assurer la sécurité de l'information en accord avec les lois et règlements ainsi que des bonnes pratiques dans le domaine ».

Cette année l'EGI fait mention de deux actions à réaliser en lien avec la sécurité des actifs informationnels.
Tout d'abord, la production d'un bilan sur les activités réalisées en sécurité informatique. Également, la mise en place d'un réseau d'alerte en sécurité informatique selon des informations qui seront fournies par le MSSS ultérieurement.

Voici les recommandations concernant l'entente de gestion et d'imputabilité 2013-2014 :

R.7.	Établir un bilan des mesures en place en matière de sécurité de l'information à l'Agence et dans les établissements
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

4.1.3. Le responsable de la sécurité des actifs informationnels

5 recommandations

En cours d'année, le RSAI est sollicité sur différents dossiers touchant la sécurité des actifs informationnels. Son expertise est requise pour orienter les projets sur les aspects impliquant les mesures de sécurité à mettre en place.

Voici les recommandations proposées par le RSAI :

R.9.	Revoir l'accès des différents fournisseurs aux actifs informationnels de l'Agence
R.10.	Mettre en place un plan de relève informatique au Technocentre
R.11.	Surveiller les équipements (applications, matériels et logiciels)
R.12.	Surveiller l'utilisation de la bande passante et l'accès aux sites malveillants
R.13.	Établir une vigie sur les meilleurs pratiques en sécurité informatique

4.1.4. Le test d'intrusion réalisé au Technocentre

3 recommandations

Un test d'intrusion réalisé au Technocentre au mois de novembre 2012 a soulevé certaines failles pour lesquelles des interventions ont déjà été réalisées et d'autres sont à venir afin de réduire les risques. Le test fait ressortir les points positifs suivants :

- Mises à jour appliqués
- Plusieurs niveaux de sécurité avec les codes d'utilisateurs ayant des privilèges élevés (administrateurs de réseau)

Voici les recommandations concernant le test d'intrusion réalisé au Technocentre :

R.14.	Créer des divisions logiques sécurisées entre les projets
R.15.	Appliquer les mises à jour aux logiciels spécifiés suite au test d'intrusion
R.16.	Harmoniser et diffuser un politique de mots de passe

4.1.5. L'auditeur externe (2011 et 2013)

6 recommandations

En 2011, l'auditeur externe a fait quelques observations sur la sécurité et a formulé les recommandations énoncées dans le tableau ci-dessous. En 2012 et 2013, des actions ont été réalisées afin de se conformer aux recommandations énoncées par l'auditeur externe.

Voici les recommandations provenant de l'auditeur externe :

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)
R.18.	Réviser les accès d'administrateurs de domaine afin que chaque compte est nominatif et nécessaire aux opérations
R.19.	Approbation des privilèges d'accès aux applications et la révision de ceux-ci devraient être effectués par une personne distincte n'ayant pas les privilèges de gestion
R.20.	Activer les accès d'un fournisseur seulement lorsqu'une demande est approuvée par l'informatique conjointement avec le Technocentre
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
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

5. Plan d'action 2013-2014

Suite aux différentes observations soulevées par l'auditeur externe, aux 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, ainsi que les résultats du test d'intrusion réalisé au Technocentre de Montréal et dans un souci d'amélioration continue, voici les actions de sécurité prévues à l'Agence pour l'année 2013-2014.

Dans son plan d'action, le responsable de la sécurité des actifs informationnels portera une attention particulière au Technocentre régional de Montréal. La nature des actifs (données nominatives et cliniques) nécessite la mise en place des recommandations afin de réduire les risques appréhendés.

R.1. **Identifier le log du système d'exploitation permettant d'identifier les accès et les tentatives infructueuses (Pavillon Lafontaine)**

Action
Mettre en place un outil permettant d'identifier dans les journaux d'événements les accès et les tentatives infructueuses (septembre 2013)
Direction
Direction du financement, de la performance et des technologies de l'information (Coordination de l'informatique et support aux usagers)

R.2. **Mettre en place un programme de sensibilisation à la sécurité des actifs informationnels pour le personnel des technologies de l'information**

Action
Développer un programme de sensibilisation spécifique au personnel travaillant en technologie de l'information (2013-2014)
Direction
Direction générale (RSAI)

R.3. **Prévoir un mécanisme de protection pour les ordinateurs portatifs ainsi que les appareils mobiles**

Action
Rechercher les différents mécanismes disponibles permettant la protection des données contenues sur le disque rigide des appareils portatifs ainsi que sur les appareils mobiles (2013-2014)
Direction
Direction générale (RSAI)

R.4. **Remplacer le registre papier par un système à carte magnétique pour plus d'imputabilité (Siège social et Pavillon Lafontaine)**

Actions

Évaluer les coûts liés à l'ajout d'un lecteur de carte magnétique pour le siège social et la Pavillon Lafontaine (septembre 2013)

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 (réalisation en décembre 2013)

Directions

Direction du financement, de la performance et des technologies de l'information (Coordination de l'informatique et support aux usagers)

Direction du secrétariat général, de l'administration, des ressources humaines et des communications (Coordination des RH internes, planification organisationnelle et services techniques)

R.5. **Effectuer une vérification bisannuelle de l'inventaire des logiciels installés**

Actions

Mettre en place un processus formel de gestion des licences (Acquisition, installation, désinstallation, etc.) (2013-2014)

Mettre en place un système d'extraction (liste) des logiciels installés sur les ordinateurs et implanter un processus de contrôle biannuel (2014-2015)

Direction

Direction du financement, de la performance et des technologies de l'information (Siège social, Pavillon Lafontaine et Technocentre)

R.6. **Installer des gicleurs dans la salle des serveurs (Pavillon Lafontaine)**

Action

Faire l'analyse du risque sachant que les actifs critiques sont déplacés vers le Technocentre versus investir dans la salle en décroissance (décembre 2013)

Directions

Direction du financement, de la performance et des technologies de l'information (Coordination de l'informatique et support aux usagers)

Direction du secrétariat général, de l'administration, des ressources humaines et des communications (Coordination des RH internes, planification organisationnelle et services techniques)

R.7. **Établir un bilan des mesures en place en matière de sécurité de l'information à l'Agence et dans les établissements**

Action
Déposer au conseil d'administration de l'Agence le bilan annuel 2011-2013 (septembre 2013)
Directions
Direction générale (RSAI)

Direction du financement, de la performance et des technologies de l'information (Coordonatrice régionale de la sécurité des actifs informationnels)

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**

Action
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 (2013-2014)
Directions
Direction générale (RSAI)

Direction du financement, de la performance et des technologies de l'information (Coordonatrice régionale de la sécurité des actifs informationnels)

R.9. **Revoir l'accès des différents fournisseurs aux actifs informationnels de l'Agence**

Action
Mettre en place une politique de gestion des accès aux fournisseurs qui va appuyer une directive interne déjà existante au Technocentre (septembre 2013)
Directions
Direction générale (RSAI)

Direction du financement, de la performance et des technologies de l'information (Technocentre)

R.10. **Mettre en place un plan de relève informatique au Technocentre**

Actions
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) (2013-2014)

Direction
Direction du financement, de la performance et des technologies de l'information (Technocentre)

R.11. **Surveiller les équipements (applications, matériels et logiciels)**

Action
Poursuivre l'implantation de l'outil de journalisation *syslog-ng* au Technocentre régional de Montréal sur les équipements de type Windows
Direction
Direction du financement, de la performance et des technologies de l'information (Technocentre)

R.12. **Surveiller l'utilisation de la bande passante et l'accès aux sites malveillants**

Actions
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 (Juin 2013)

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 (décembre 2013)

Directions
Direction du financement, de la performance et des technologies de l'information (Siège social, Pavillon Lafontaine et Technocentre)

Direction générale (RSAI)

R.13. **Établir une vigie sur les meilleurs pratiques en sécurité informatique**

Action
Surveiller durant la prochaine année :

- 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).

Direction
Direction générale (RSAI)

R.14. **Créer des divisions logiques sécurisées entre les projets**

Action
Limiter les accès logiques aux équipements situés dans la salle informatique du Technocentre
Une demande budgétaire a été réalisée afin de procéder à l'acquisition des équipements nécessaires (2013-2014)
Direction
Direction du financement, de la performance et des technologies de l'information (Technocentre)

R.15. **Appliquer les mises à jour aux logiciels spécifiés suite au test d'intrusion**

Action
Installer les correctifs nécessaires aux logiciels spécifiés afin de corriger les différentes vulnérabilités (2013-2014)

Direction
Direction du financement, de la performance et des technologies de l'information (Technocentre)

R.16. **Harmoniser et diffuser une politique de mots de passe**

Action
Rédiger une politique sur la gestion des mots de passe (Septembre 2013)
Direction
Direction générale (RSAI)

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)**

Action
Ajouter l'application GRF et GRM au processus annuel de révision des accès aux applications
Directions
Direction du secrétariat général, de l'administration, des ressources humaines et des communications (Coordination des finances et des approvisionnements)

Direction du financement, de la performance et des technologies de l'information (Coordination de l'informatique et support aux usagers)

R.18. **Réviser les accès d'administrateurs de domaine afin que chaque compte est nominatif et nécessaire aux opérations**

Action
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 (Juin 2013)
Direction
Direction du financement, de la performance et des technologies de l'information (Coordination de l'informatique et support aux usagers)

R.19. **Approbation des privilèges d'accès aux applications et la révision de ceux-ci devraient être effectués par une personne distincte n'ayant pas les privilèges de gestion**

Action
Élaborer un processus de travail d'ici le 31 mars 2014 qui permettra de documenter les approbations et la révision des 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.

Direction
Direction du secrétariat général, de l'administration, des ressources humaines et des communications (Coordination des finances et des approvisionnements)

R.20. **Activer les accès d'un fournisseur seulement lorsqu'une demande est approuvée par l'informatique conjointement avec le Technocentre**

Action
Arrimer cette recommandation avec celle concernant l'accès des différents fournisseurs aux actifs informationnels de l'Agence

Directions
Direction du secrétariat général, de l'administration, des ressources humaines et des communications (Coordination des finances et des approvisionnements)

Direction du financement, de la performance et des technologies de l'information (Coordination de l'informatique et support aux usagers ainsi que le Technocentre)

Direction générale (RSAI)

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**

Actions
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 (2013-2014)

Directions
Direction du secrétariat général, de l'administration, des ressources humaines et des communications (Coordination des finances et des approvisionnements)

Direction du financement, de la performance et des technologies de l'information (Coordination de l'informatique et support aux usagers)

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**

Action
Négocier et signer une entente de service afin de définir les services à fournir, les modalités et responsabilités de chaque partie impliquée (2013-2014)

Directions
Direction du secrétariat général, de l'administration, des ressources humaines et des communications (Coordination des finances et des approvisionnements)

Direction du financement, de la performance et des technologies de l'information (Coordination de l'informatique et support aux usagers ainsi que le Technocentre)

6. Conclusion

La sensibilisation sur la sécurité des actifs informationnels doit se faire de façon continue afin que l'acteur le plus important, c'est-à-dire l'utilisateur, agisse de façon responsable. Ainsi, les utilisateurs se questionnent de plus en plus sur les mesures qui peuvent être mises en place afin d'améliorer la sécurité des actifs informationnels détenus par l'Agence de Montréal dans ses différentes installations. Cela permet également à l'utilisateur ainsi qu'au personnel des technologies de l'information de mieux réagir lorsque ceux-ci font face à un incident touchant la sécurité (incident éthique ou technologique). La coopération ainsi qu'une bonne communication avec toutes les personnes utilisant les actifs informationnels sont nécessaires afin que celles-ci signalent les situations pouvant affecter la sécurité des données.

La sécurité des actifs informationnels est un domaine en constant changement avec l'utilisation des nouvelles technologies qui modifient grandement les façons d'utiliser les actifs informationnels, surtout ceux en format électronique. Les nouvelles technologies apportent également de nouveaux risques aux actifs informationnels. C'est pour cela qu'il est important de faire une analyse de risques qui permettra ainsi de mettre en place les mesures nécessaires afin de réduire les risques.

La disponibilité des technologies de l'information modifie de façon importante les pratiques cliniques en y introduisant une plus grande accessibilité, partage et circulation de l'information clinique notamment. La mobilité des applications permet maintenant aux cliniciens une plus grande liberté de pratique en réduisant le temps passé à transcrire des informations. Ces nouveaux développements doivent être soutenus par un encadrement où la sécurité doit être omniprésente.

Un des plus grands enjeux de cette démarche sera de concilier les bénéfices d'une plus grande accessibilité de l'information clinique avec les limites d'un cadre de gestion de la sécurité des actifs informationnels qui soit à la fois rigoureux et adapté à la réalité actuelle du réseau montréalais. La région de Montréal, en tant que milieu universitaire de pointe et d'innovation, constitue un terreau propice au développement en matière de technologies de l'information. Le déploiement du dossier clinique informatisé OACIS dans les établissements et la mise en place de dossiers médicaux électroniques dans les cliniques médicales GMF-CR et CRI sont des réalisations concrètes qui alimentent la réflexion pour mettre en place les meilleures pratiques en matière de sécurité dans la démarche montréalaise d'informatisation.

L'émergence de nouveaux moyens et de nouvelles plateformes de communications jumelées aux systèmes et aux applications en place rendent encore plus aigus les besoins de protection et de sauvegarde des 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.

L'Agence doit maintenir sa vigilance et son implication dans les différents sites afin d'assurer la protection de ses actifs.

LISTE DES ANNEXES

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;

Intervenant/entité	Rôles/Responsabilités
	• 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 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,

Intervenant/entité	Rôles/Responsabilités
	après approbation de la PDG et du conseil d'administration, les soumettre au coordonnateur régional de la sécurité des actifs informationnels.
Direction du financement, de la performance et des technologies de l'information	• 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; • 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;

Intervenant/entité	Rôles/Responsabilités
	• 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 du secrétariat général, de l'administration, des ressources humaines et des communications	• 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.

Mesures	Résultats
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.
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 24 et 26 avril 2012

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.

2.2. Procéder à l'installation de l'antivirus sur le serveur de développement du siège social dans les meilleurs
3.2. Adopter la même procédure de sécurité du transport des archives avec le Technocentre.
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.
9.1. - Entreposer les documents importants (contrats, médias, …) dans la voûte au 2e étage.
- Numériser et sauvegarder tous les documents importants.

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.

3.1. Sécuriser les sauvegardes sur site externe
3.2. Adopter la même procédure de sécurité du transport des archives avec l'Agence.
4.3. Effectuer des tests mensuels de recouvrements du système.
5.1. Rédiger un document présentant le processus d'installation des logiciels sur les postes de travail.
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.

2.2. Rechercher avec la SOGIQUE et TrendMicro la meilleure solution antivirus pour la plateforme Macintosh.
5.1. Rechercher un logiciel pour automatiser la gestion de l'inventaire.
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.
13.2. Prévoir un mécanisme de protection pour les ordinateurs portatifs.
14.1. Augmenter la longueur des mots de passe à 8 caractères et complexifier sa composition.
14.3. Identifier le log du système d'exploitation permettant d'identifier les accès et les tentatives infructueuses.

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

Composition du comité en date du 6 décembre 2012

Personnes désignées	Titre d'emploi et direction
M. Jean Béliveau	Spécialiste en procédés administratifs, Direction des affaires cliniques, médicales et universitaires
M. Christian Bertrand	Coordonnateur, Direction du financement, de la performance et des technologies de l'information
Mme Loraine Desjardins	Adjointe à direction générale, Direction générale
Mme Caroline Dusablon	Agente de planification, Direction du secrétariat général, de l'administration, des ressources humaines et des communications
M. Denis Hébert	Chef de service, Direction du secrétariat général, de l'administration, des ressources humaines et des communications
M. Stéphane Gagnon	Responsable de la sécurité des actifs informationnels, Direction générale
Mme Hélène Gendron	Chef de service, Direction du financement, de la performance et des technologies de l'information
Mme Lydia Ingenito	Directrice adjointe, Direction des programmes-services
Mme Brigitte Lagacé	Commissaire régionale aux plaintes et à la qualité des services
M. Serge Laniel	Coordonateur, Direction du financement, de la performance et des technologies de l'information
M. Roger Martin	Conseiller-cadre, Direction des immobilisations, des technologies médicales et services techniques

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.

Annexe 5 - 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.
CRSAI	Coordonatrice régionale de la sécurité des actifs informationnels
DIC	Disponibilité, Intégrité et Confidentialité (les 3 principes fondamentaux en sécurité de l'information)
DFPTI	Direction du financement, de la performance et des technologies de l'information
DSGARHC	Direction du secrétariat général, de l'administration, des ressources humaines et des communications
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

Agence de la santé
et des services sociaux
de Montréal
Québec