Agence de la santé et des services sociaux de Montréal

Bilan de la sécurité des actifs informationnels 2005-2011

APPROUVÉ
PAR
LE CONSEIL D'ADMINISTRATION DE
L'AGENCE DE LA SANTÉ ET DES SERVICES SOCIAUX DE MONTRÉAL
LE 14 FÉVRIER 2012

Québec

Bilan de la sécurité des actifs informationnels 2005 2011

Décembre 2011

Agence de la santé et des services sociaux de Montréal
Québec

Coordination
Loraine Desjardins, adjointe au directeur, ressources humaines, information, planification et affaires juridiques

Recherche et rédaction
Ralès Bessard, officier de sécurité
Loraine Desjardins

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 des ressources humaines, de l'information, de la planification
Et des affaires juridiques de l'Agence de la santé et des services sociaux de Montréal
Janvier 2012

ISBN 978-2-89510-617-3 (version imprimée)
ISBN 978-2-89510-618-0 (PDF)

Dépôt légal - Bibliothèque et Archives nationales du Québec, 2012

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

TABLE DES MATIÈRES

PRÉAMBULE

Le présent bilan de la sécurité des actifs informationnels de l'Agence de la santé et des services sociaux est présenté pour la première fois au conseil d'administration de l'Agence et couvre une période qui s'étend de 2005 à 2011. Dorénavant, un bilan annuel de la sécurité sera présenté aux administrateurs de l'Agence pour approbation. En matière de sécurité des actifs informationnels les agences régionales sont considérées comme des établissements. Elles sont donc soumises aux mêmes règlements et doivent donc se conformer aux préceptes qui encadrent la sécurité des actifs informationnels.

Le document présente 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

Il décrit les réalisations et les mesures qui ont été implantées par les équipes de l'Agence au cours des cinq dernières années pour protéger ses actifs informationnels dans les quatre sites physiques qu'elle occupe actuellement.

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

Une série d'annexes vient compléter l'information.

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)

I. 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, ceux-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.

Ce document a pour objectif de communiquer les attentes, les obligations et les rôles de chacun des intervenants en matière de sécurité des actifs informationnels. Le Cadre global qui propose 64 mesures de sécurité (voir annexe 1) est appelé à évoluer et à s'adapter aux différents environnements de notre réseau.
Il est nécessaire de souligner que ce cadre de gestion vise aussi bien les informations de nature électronique (ou numérique) contenues dans les actifs informationnels appartenant aux organismes du RSSS que les impressions sur support papier.

La priorité du MSSS est de mettre en place l'ensemble des mesures obligatoires prévues dans le Cadre global. Pour ce faire, six étapes sont identifiées afin de produire les livrables attendus qui attestent de la conformité des mesures implantées. Depuis 2005, l'Agence de Montréal a franchi ces six étapes qui lui ont permis de réaliser des actions et de produire les documents prescrits par le CGAI soit :

Étape 1
Politique de sécurité pour établir et encadrer la sécurité des actifs informationnels afin de mettre en place des contrôles de sécurité et de diminuer les risques à un niveau jugé acceptable;
Étape 2
Sessions de sensibilisation et de formation continue à l'ensemble du personnel ;
Étape 3
Implantation des 15 mesures prioritaires provenant du Cadre global et représentant les exigences minimales en terme de sécurité pour les établissements ;
Étape 4
Inventaire et catégorisation des actifs informationnels ;
Étape 5
Analyse de risque et d'impact ;
Étape 6
Plan directeur.

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) et
- 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 sites physiques différents. 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 :

1- 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) ;
2- Technocentre régional (4835, rue Christophe-Colomb, relève OACIS et système d'imagerie) ;
3- La Direction de santé publique (1301, rue Sherbrooke est, qui est mandatée par HMR, CUSM et l'Agence pour la vigie et la surveillance en santé publique) ;
4- L'Agence de la santé et des services sociaux de Montréal (3725, rue St-Denis), siège social.

Il existe donc une variété de mesures qui sont appliquées afin de protéger adéquatement l'information de l'Agence de Montréal dans ses différents sites. Le bilan de ces actions est présenté aujourd'hui pour la première fois depuis les cinq premières années. C'est pourquoi une présentation générale des réalisations en matière de sécurité depuis l'année 2006 a été privilégiée. Au cours des prochaines années, un bilan annuel des actions réalisées au cours de l'année sera déposé au conseil d'administration de l'Agence.

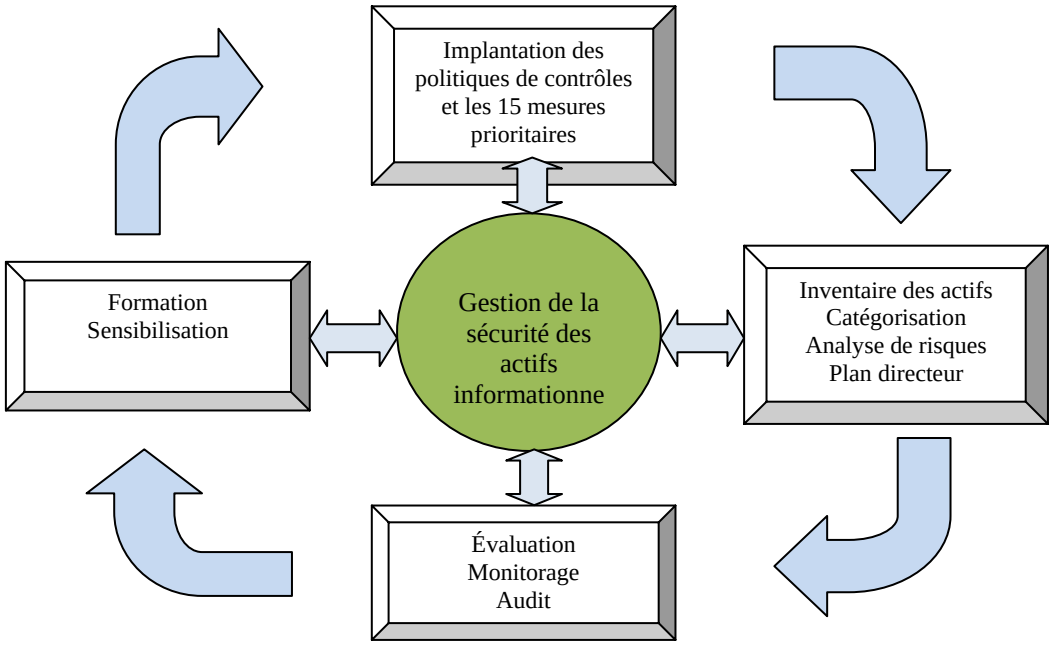


Fig. 1 Gestion de la sécurité des actifs informationnels

II. 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
Président-Directeur Général (PDG)	• Nommer le responsable de la sécurité des actifs informationnels (RSAI). Cette nomination doit être entérinée par le conseil d'administration; • S'assurer du partage des valeurs et des 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)	• Voir section 3.1
Responsable de sécurité des actifs informationnels (RSAI)	• Coordonner l'application des directives reliées à la sécurité de l'information; • Planifier et organiser les différentes activités de sensibilisation reliées à la sécurité de l'information, • Assurer le respect des directives et l'application des procédures en cas de défaillance; • Gérer les aspects relatifs à l'escalade des incidents de sécurité de l'information.
Service des Technologie de l'Information (TI)	• 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; • Tenir des inventaires sur les équipements et logiciels; • Gérer les mots de passe; • Mettre 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 présente Politique; • Mettre 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 il est détenteur; • Évaluer les risques et déterminer le niveau de protection visé; • Élaborer des contrôles non informatiques; • Voir au suivi des codes de conduite émis par le service des ressources humaines; • S'assurer que son personnel est au fait de leurs obligations découlant de la présente politique, normes et procédures de sécurité en vigueur.
Service des ressources humaines	• Informer toute nouvelle personne de ses obligations découlant de la Politique de sécurité; • Sensibiliser toute nouvelle personne 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.
Utilisateurs	• Prendre connaissance de la Politique de sécurité; • Respecter la présente Politique, normes, directives et procédures en vigueur en matière de sécurité de l'information et les autres politiques et directives y 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.

III. Bilan global des activités et des réalisations

Le démarrage des activités et des réalisations en sécurité des actifs informationnels de l'Agence a débuté en novembre 2005 avec l'embauche d'un responsable de la sécurité des actifs informationnels pour coordonner la gestion et faire le suivi à l'Agence et dans le réseau montréalais de la santé. A la suite de l'embauche, en 2007 d'un second responsable de la sécurité, la coordination régionale de la sécurité des actifs informationnels a été accordée à un responsable alors que la sécurité dans les quatre sites de l'Agence a été octroyée au second responsable de la sécurité.

Le tableau suivant présente les jalons qui ont marqué les réalisations en matière de sécurité.

Années	Réalisations
Novembre 2005	Embauche d'un responsable de la sécurité
Mai 2006	Création du comité de sécurité des actifs informationnels
Juin 2006	Élaboration de la politique de sécurité des actifs informationnels
Mai 2007	Catégorisation des actifs informationnels
Février 2008	Analyse des risques des actifs informationnels
Octobre 2008	Implantations des 15 mesures prioritaires
Avril 2009	Plan directeur
Octobre 2010	Analyse de gestion des risques majeurs
Mars 2011	Audit interne
Mai 2011	Bilan des incidents critiques
Octobre 2011	Révision du plan directeur
Décembre 2011	Bilan de la sécurité des actifs informationnels 2005-2011

1- Création d'un 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 diverses directions et services de l'Agence et il se réunit environ 4 fois par année. Il agit à titre d'aviseur conseil et participe aux orientations pour tout ce qui touche la sécurité en application du Cadre global.

Mandats :

- Agir comme rôle de conseil auprès du responsable de la sécurité des actifs informationnels (RSAI)
- Agir comme un mécanisme de coordination et de concertation qui propose des orientations et fait 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 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.
- Approuver 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.

Composition du comité en date du 22 novembre 2011

Personnes désignées	Titre d'emploi
M. Frédéric Abergel	Directeur adjoint, direction des affaires cliniques, médicales et universitaires
M. Ralès Bessard	Responsable de la sécurité des actifs informationnels
Mme Loraine Desjardins	Adjointe au directeur, direction des ressources humaines, de l'information, de la planification et des affaires juridiques
Mme Hélène Gendron	Chef de service, systèmes d'information et de l'informatique – St-Denis
Mme Renée-Marthe Giard	Responsable, secteur administration, direction de la santé publique
Mme Sylvie Hubert	Chef de service, Gestion de l'information
Mme Brigitte Lagacé	Commissaire régionale aux plaintes et à la qualité des services
M. Serge Laniel	Adjoint, services au réseau, Technologies et systèmes d'information - Technocentre
M. Vincent Lehouillier	Adjoint à la direction générale, administration générale et ressources humaines
M. Roger Martin	Conseiller-cadre, gestion des immobilisations et des technologies médicales

2- Élaboration et adoption de la politique de sécurité des actifs informationnels

La politique de sécurité de l'Agence (annexe 2) a été déposée et adoptée par le conseil d'administration le 20 juin 2006. Une version actualisée est présentement en préparation.

Cette politique constitue la pierre angulaire et le fondement du programme de sécurité 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- Catégorisation des actifs informationnels

En mai 2007, un inventaire complet des actifs informationnels au sein de l'Agence a été réalisé dans le but d'en faire la catégorisation. Cet exercice a mobilisé plusieurs personnes du service informatique interne qui ont

sollicité la collaboration de tous les cadres de l'Agence. Cette démarche s'est échelonnée sur une période de huit (8) mois. Cela a permis d'identifier les actifs informationnels pour lesquels une analyse de risques est nécessaire afin de cibler les activités à réaliser.

En se basant sur le Cadre global de gestion des Actifs informationnels (CGGAI) – volet sécurité, deux catégories d'actifs ont été inventoriées :

1. Actifs informationnels en format électronique, incluant les documents électroniques (de type texte, Excel, Word, Texte, MSProject, Powerpoint ou même d'autres formats), les applications et les bases de données.
2. Actifs informationnels en format papier, incluant les documents issus des différents processus et détenus par les unités administratives.

Afin de respecter les principes de la sécurité de l'information et faciliter la phase d'analyse des risques, on a fourni pour chaque actif, sa cote en DIC (Disponibilité, Intégrité et Confidentialité), ce qui définit sa valeur. Aussi, on a relevé pour chaque actif, le nom de son détenteur ou propriétaire, sa localisation, et finalement la présence de renseignements personnels (PRP) à l'intérieur de l'actif informationnel.

En ce qui concerne la phase d'analyse de risques, on ne retiendra que les actifs dont la valeur de la disponibilité et/ou l'intégrité et/ou la confidentialité est supérieure ou égale à 3. Cette démarche a aidé à se concentrer uniquement sur les actifs les plus critiques.

Également, il est à noter que l'étape de catégorisation est un processus continu et par conséquent il doit faire l'objet de réévaluations périodiques, afin de prendre en compte les changements organisationnels et technologiques de l'Agence ainsi que l'évolution des menaces et des risques inhérents aux actifs informationnels de l'établissement.

Catégorisation : Échelle des valeurs

Principe	Valeur de l'actif 1 = bas, 2 = moyen, 3 = élevé, 4 = critique
D - Disponibilité	Valeur 1 à 4
I - Intégrité	Valeur 1 à 4
C - Confidentialité	Valeur 1 à 4

4- Analyse de risques

En février 2008, à la suite de l'exercice de catégorisation des actifs, une analyse de risques et un état de la situation ont été réalisés sur tous les actifs dont le DIC est égal ou supérieur à 3.

L'analyse de risques consiste à identifier les principales menaces liées à l'utilisation et à la manipulation des actifs informationnels tandis qu'un état de la situation actuelle consiste à effectuer une revue approfondie des contrôles permettant de protéger lesdits actifs. La combinaison de ces deux étapes permet d'élaborer le plan directeur.

5- Implantation des 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 sites 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. La Direction de site santé publique et l'Agence (3725, rue St-Denis) utilisent un fournisseur externe pour l'entreposage des cassettes 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, a 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, homologué, 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	Pour la prévention contre le feu, les sites du Technocentre et

l'extinction des incendies	Saint-Denis sont conformes en ayant des détecteurs de fumée, des gicleurs et un système relié à une centrale. La salle de la DSP ne se conforme pas selon le 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-Mise en place et vérification de politique des comptes usager, profils et codes d'accès, gestion des mots de passe et journaux	Une politique de gestion des comptes usager et des mots de passe est en place et un journal d'accès sont maintenus pour assurer l'imputabilité.
15-Maintenance des comptes usager	Une procédure et des fiches d'installation sont utilisées en collaboration avec les ressources humaines afin de s'assurer de la mise à jour constante des informations concernant les employés de l'Agence.

6- Plan directeur

Réalisé en avril 2009, le plan directeur de sécurité 2009-2012 (voir annexe 3) présente les actions à réaliser en ordre de priorité et l'estimé des efforts à cette fin. Ces actions sont les projets et les mesures qui devront être implantées à court terme, à moyen terme et à long terme pour réduire la probabilité de matérialisation ou les impacts des principaux risques à un niveau jugé acceptable. Il prévoit également un espace afin de consigner l'estimation des coûts requis pour l'acquisition de logiciels et d'équipements de sécurité. Une mise à jour de ce document en 2011 a permis de préciser les cibles d'actions pour 2011-2012.

7- Analyse des risques majeurs

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

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 entreprises afin d'atténuer ou éliminer ces risques.

Risques	Mesures atténuantes
Sécurité des données	Mise en place de la sécurité et implication plus accrue du RSAI dans le processus d'implantation des nouveaux projets. Acquisition d'un équipement de stockage pour centraliser et sécuriser les données sensibles à la DSP. 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 Saint-Denis et le TCR.
Intrusions à son réseau informationnel	Consolidation des journaux de sécurité par le déploiement d'un outil de journalisation au TCR.
Fuite de renseignements	Test d'un outil de contrôle d'accès et de filtrage Internet pour le site Saint-Denis.
Absence de relève du réseau de télécommunications au Technocentre	Mise en place de façon d'une infrastructure de relève pour les applications critiques.

8- Audit interne sur les 15 mesures prioritaires du Cadre global

En mars 2011, un premier audit interne été réalisé dans les 4 sites de l'Agence dans le but de valider l'atteinte des exigences liées à l'implantation des15 mesures prioritaires du Cadre global. Pour ce faire, un comité a été formé composé des auditeurs suivants : Mme Louise Francoeur (analyste informatique et représentante sécurité, DSP), M. Stéphane Gagnon (analyste informatique, Saint-Denis) et M. Martin Villeneuve (analyste informatique et représentant sécurité, 2 TCRs) ainsi que M. Ralès Bessard (responsable à la sécurité des actifs informationnels).

Lors de ce processus, des questions de base ont été posées et certaines preuves demandées pour fin de vérification. Un rapport a été déposé, accompagné de recommandations (annexe 4) pour chaque site afin de corriger les lacunes identifiées. Un tel exercice serait effectué de façon régulière, aux deux ans et pour ce faire, un auditeur externe serait mandaté pour effectuer cette vérification en toute impartialité.

9- Bilan des incidents critiques

Depuis mai 2011, une liste des incidents critiques est demandée par le Responsable de la sécurité des actifs informationnels (RSAI) aux responsables des 4 sites. De façon trimestrielle, un rapport sera créé pour chaque incident critique survenu durant cette période. Des mesures spécifiques ont été réalisées afin d'atténuer et/ou éliminer les risques identifiés. Ce rapport sera envoyé au RSAI pour vérifier les causes et s'assurer que les correctifs et solutions apportés soient efficaces et à long terme.

Un incident critique peut affecter plusieurs services et/ou a un impact majeur sur la continuité des affaires de l'Agence.

Quelques exemples d'incidents critiques:

- Dysfonctionnement du système d'information OACIS ;
- Propagation d'un virus informatique au niveau de l'organisation ;
- Arrêt du système de messagerie Lotus Notes ;
- Piratage du site Web de l'Agence ;
- Etc.

Un incident peut être technique ou éthique. Sa criticalité est définie par son impact sur la continuité des services offerts par l'Agence.

IV. Recommandations du vérificateur informatique

Lors de sa visite annuelle à l'Agence (site 3725, rue Saint-Denis) en Janvier 2011, le vérificateur informatique a fait quelques observations sur la sécurité et a formulé les recommandations suivantes :

- **Dans la gestion des accès des utilisateurs internes :**
  L'application Espresso Paie n'exige pas que les mots de passe de utilisateurs soient modifiés périodiquement tel qu'exigé à la mesure 4.2.1 du Cadre global de gestion. Le mot de passe n'est pas composé d'au moins 8 caractères, tel qu'exigé à la mesure 4.2.2 du Cadre global de gestion.

  Action entreprise:
  Contacter le fournisseur de l'application LOGIBEC pour arrimer ce point avec les politiques de sécurité d'accès établies à l'Agence et vérifier si ces pratiques existent dans les autres établissements.

- **Dans la mise en place d'une saine gestion en sécurité** :
  Le bilan annuel de l'organisme concernant la sécurité de ses actifs n'a pas été entériné par le conseil d'administration de l'établissement tel que stipulé à la mesure 2.1 du cadre global de gestion.

  Action entreprise:
  Tel que prévu dans la politique de sécurité de l'Agence, un bilan annuel de sécurité sera soumis au conseil d'administration cette année et annuellement par la suite.

- **Dans la mise en place d'un environnement de sécurité efficace**
  La salle des serveurs n'est pas dans un local permettant de voir les faits et gestes du personnel autorisé présent à l'intérieur du local, tel que stipulé à la mesure 4.11 du cadre global de gestion.

  Action entreprise:
  Une soumission a été demandée pour l'acquisition d'une caméra dans la salle.

V. Plan d'action 2011-2012

Suite aux observations soulevées par le vérificateur informatique, aux faiblesses notées par l'audit interne, par les commentaires du RSAI délégué et dans un souci d'amélioration continue, voici les actions de sécurité prévues à l'Agence pour l'année 2011-2012.

Risques	Mesures	État d'achèvement
- Bris et/ou indisponibilité des applications, logiciels et équipements - Négligences et erreurs humaines	Améliorer les mécanismes de révision des applications, systèmes et équipements par l'enrichissement et la mise à jour de la documentation et des procédures d'exploitation.	En continu
- Bris dans les applications, logiciels et équipements	Terminer la 1ère phase d'implantation de l'outil de journalisation *syslog-ng* au Technocentre et commencer la 2e phase d'installation et d'implantation à la DSP et Saint-Denis	1ère phase réalisée en mars 2011, 2e phase début 2012
- Utilisation excessive de la bande passante - Accès aux sites malveillants	Acquérir un logiciel de contrôle et de filtrage internet pour les sites DSP et Saint-Denis	Installé à la DSP Fin des tests, début 2012 sur Saint-Denis
- Utilisation inappropriée ou non autorisée des équipements	Installer une mini-caméra de surveillance pour visualiser les faits et gestes des intervenants dans la salle informatique de Saint-Denis	Soumission reçue, achat à faire.
- Accès non autorisés dans l'application Espresso Paie	Évaluer et corriger la robustesse des mots de passe	En cours
- Mauvaise utilisation de l'internet et des médias sociaux	Analyser et faire un rapport sur l'utilisation des médias sociaux et leurs impacts sur l'Agence.	Non débuté
- Non-conformité au cadre global	Réaliser l'audit interne annuel sur les contrôles de sécurité basés sur les 15 mesures prioritaires du Cadre global.	Complété en avril 2011
- Ignorance des rôles et responsabilités en matière de sécurité de l'information	Faire un sondage aux employés sur la connaissance de la sécurité des actifs informationnels.	En cours
- Mauvaise utilisation des actifs informationnels	Formation et sensibilisation des employés/cadres en continu.	En continu

VI. Pistes d'améliorations

La réalisation du bilan sur la sécurité des actifs informationnels de l'Agence a permis de constater qu'un grand nombre de mesures sont en place dans chacun des sites de l'Agence pour assurer la sécurité de l'information qui est utilisée quotidiennement. Bien qu'un grand nombre de personnes soient conscientes de l'importance de maintenir et de préserver la sécurité de nos informations, nous constatons qu'il nous faut continuer à transmettre nos messages de prévention et de sensibilisation à l'ensemble de notre personnel.

L'amélioration de nos processus et de nos actions doit se poursuivre avec toute la détermination et la vigilance souhaitées. Pour ce faire, nous avons réuni les mesures qui permettent d'enrichir nos façons de faire et de maximiser nos actions :

- Un bilan annuel sera soumis pour informer les autorités de l'état global de la sécurité à l'Agence.
- Une démarche de recrutement est en cours pour assurer une représentativité de toutes les directions au comité de sécurité des actifs informationnels
- Désormais, des rapports d'incidents critiques seront fournis sur une base régulière au RSAI pour assurer la mise en place de mesures correctives à long terme.
- Des audits annuels permettront de vérifier si les mesures en place satisfont les exigences gouvernementales.
- Les responsables des projets informationnels et cliniques seront rencontrés pour insister sur l'importance d'intégrer la sécurité dès le démarrage.

VII. Conclusion

Un important et nécessaire travail de sensibilisation auprès des différentes équipes, de conciliation des responsables des différents sites et de documentation et de recherche pour se conformer aux exigences du Cadre global a été réalisé au cours des dernières années. L'agence de Montréal dispose maintenant d'une infrastructure de sécurité lui permettant de protéger minimalement ses actifs et d'identifier les faiblesses dans une perspective d'amélioration continue.

De nouveaux enjeux se dessinent avec les nouvelles plateformes technologiques qui facilitent l'intégration des informations cliniques et des données utiles aux directions de l'Agence. 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 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 et de plus en plus 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'Agence est sur la bonne voie et doit maintenir sa vigilance et son implication dans les différents sites pour toujours mieux protéger ses actifs.

VIII. LISTE DES ANNEXES

Annexe 1 : Les 64 mesures du Cadre Global de Gestion des Actifs Informationnels (CGGAI)

MESURES *	EXIGENCES CAI[1]
PLANS D'ACTION	
Classification des actifs informationnels	
1. Les organismes du RSSS doivent produire et tenir à jour l'inventaire de leurs actifs informationnels, la liste des détenteurs de ces actifs, la classification de ces actifs en fonction de leur valeur et leur sensibilité ainsi que les plans d'action établis pour les protéger.	
Évaluation des risques et des menaces	
2. Les organismes du RSSS doivent évaluer, périodiquement mais aussi au besoin, les risques et les menaces pour tous leurs actifs informationnels afin de tenir compte des incidents survenus, tels que les intrusions et la détection de virus, et des modifications significatives de l'environnement technologique, comme le raccordement au RTSS ou le déploiement de nouvelles applications.	
MESURES DE SÉCURITÉ	
3. Toute information portant sur des processus ou des mesures touchant la sécurité des actifs informationnels doit être gérée de façon confidentielle par l'organisme.	
Sécurité physique	
• **Pour l'emplacement des installations et du matériel**	
4. Les locaux où se trouvent les ordinateurs centraux, les mini-ordinateurs, les serveurs des réseaux locaux, le matériel de télécommunications et autres actifs informationnels doivent : − être situés dans des endroits protégés contre les catastrophes naturelles (ex. : verglas, inondations) ou accidentelles (ex. : bris d'aqueduc ou de tuyauterie, surchauffe, déclenchement de gicleurs) ; − être protégés par des mécanismes de contrôle d'accès ; − être munis de systèmes de chauffage, de ventilation et de climatisation conformes aux normes recommandées par les fournisseurs ; − être munis d'un système d'alimentation électrique sans interruption et d'un système de protection contre les incendies ; − permettre de voir les faits et gestes du personnel autorisé présent à l'intérieur du local (aire ouverte).	Mesure 6
5. Les équipements, ce qui comprend les imprimantes, les photocopieurs et les télécopieurs, doivent être placés de façon à éviter toute utilisation et observation non autorisées.	Mesure 5.3
• **Pour le contrôle de l'accès aux locaux**	
6. L'accès aux locaux où se trouvent les ordinateurs centraux, les mini-ordinateurs, les serveurs des réseaux locaux, le matériel de télécommunications et autres actifs informationnels doit être limité au strict minimum et réservé aux personnes autorisées uniquement.	Mesure 6

1 Voir le document produit par la Commission d'accès à l'information en 1992 et intitulé *Exigences minimales relatives à la sécurité des dossiers informatisés des usagers du RSSS*.

MESURES	EXIGENCES CAI[1]
7. Une liste des personnes autorisées à accéder à ces locaux doit être constituée. Outre le nom de ces personnes, la liste comporte l'énumération des tâches autorisées pour chacune d'entre elles et la durée habituelle de leur intervention ; cette liste doit être mise à jour périodiquement.	
8. Un mécanisme de contrôle de l'entrée et de la sortie des personnes qui accèdent aux locaux sécurisés doit être mis en place.	
9. Le personnel externe (ex. : fournisseurs, consultants, tiers n'étant pas des employés) chargé de l'entretien et de la réparation des équipements ou de tout autre type d'intervention permise doit être accompagné par une personne autorisée.	
• **Pour le matériel informatique (incluant les portables)**	
10. L'inventaire des équipements, précisant la localisation et l'assignation principale de ces équipements doit être constitué et tenu à jour.	
11. La configuration de base des équipements installés doit être définie et tenue à jour.	
12. Le registre de l'entretien des équipements doit être constitué et tenu à jour.	
13. Les équipements déclarés en surplus ou mis au rebut doivent être exempts d'information électronique avant leur abandon.	
14. Les renseignements nominatifs ou de nature sensible contenus sur les supports magnétiques (disque dur, disquette, CD-ROM) que l'on désire éliminer doivent être détruits de façon à ce que leur caractère confidentiel soit protégé.	Mesure 2.7
15. L'information contenue sur tout équipement à déplacer doit, au préalable, être analysée et, le cas échéant, éliminée.	
16. Des procédures ou des mécanismes de protection contre l'utilisation non autorisée et le vol des équipements doivent être mis en place.	
17. L'organisme doit instaurer une procédure obligatoire pour autoriser la sortie d'équipements hors de ses installations.	
Sécurité logique	
• **Pour le contrôle de l'accès aux actifs informationnels**	
18. Un mécanisme d'identification et d'autorisation doit être mis en place afin de limiter aux seules personnes autorisées l'accès aux actifs informationnels.	Mesures 1.1, 1.4 et 1.5
19. L'autorisation d'avoir accès aux actifs informationnels à l'aide d'un identifiant doit être suspendue après un nombre prédéterminé (cinq au maximum) d'erreurs d'inscription du mot de passe par l'utilisateur.	Mesure 1.9
20. Les privilèges relatifs à d'accès doivent être accordés et mis à jour selon les tâches et responsabilités de chaque utilisateur. L'accès doit être révoqué ou suspendu lorsque l'utilisateur s'absente pour une période de plus de six semaines ou quitte définitivement l'organisme. L'outil de gestion des privilèges informatiques ou administratifs doit comporter des mécanismes permettant de réviser, de suspendre, de révoquer, de bloquer ou de radier ces privilèges en tout temps.	Mesures 1.11, 2.1, 2.8 et 13.1
21. Les privilèges d'accès accordés aux utilisateurs doivent être inscrits dans un registre maintenu à jour. L'utilisateur qui a accès à des données personnelles ou sensibles signe un formulaire par lequel il s'engage à en respecter la confidentialité.	Mesure 11.2
22. L'identifiant doit être différent pour chaque utilisateur sauf en de rares exceptions incontournables, définies et pour lesquelles les autorisations préalables ont été accordées par le responsable attitré ; ces autorisations doivent être consignées dans un registre prévu à cette fin.	Mesure 1.2
23. L'identifiant qui n'a pas été utilisé pendant une période donnée (un an au maximum) doit être désactivé ou détruit à la suite d'une vérification préalable.	Mesure 1.3

MESURES	EXIGENCES CAI[1]
24. L'application qui accède à une autre application doit être considérée comme un utilisateur et être assujettie aux mesures applicables aux utilisateurs.	
• **Pour l'authentification**	
25. Des mesures doivent être mises en place pour contrôler et protéger l'authentifiant de l'utilisateur.	Mesures 1.7 et 1.10
26. Après une période d'inactivité prédéterminée (une heure au maximum), le système doit automatiquement redemander l'authentifiant de l'utilisateur ou mettre un terme à la session de travail.	Mesure 5.2
27. Le système doit protéger la confidentialité des données servant à l'authentification des utilisateurs en empêchant, entre autres, l'affichage et l'impression de ces informations.	Mesure 1.7
28. Le mot de passe comprendra des lettres, des chiffres ou des caractères spéciaux. Il doit être composé d'au moins 8 caractères et être changé au moins une fois tous les 90 jours. De plus, l'historique des 10 derniers mots de passe doit être conservé afin de s'assurer que les nouveaux mots de passe diffèrent des précédents.	Mesures 1.6 et 1.8
• **Pour l'irrévocabilité des actes**	
29. Tous les accès doivent être journalisés. La journalisation doit obligatoirement permettre de connaître l'identité de l'utilisateur, le nom du fichier auquel cet utilisateur a eu accès, l'acte qu'il a accompli (création, lecture, impression, modification ou destruction d'un dossier), le code de transaction ou le nom du programme, la date et l'heure de l'accès. La journalisation doit également consigner ces renseignements au moment d'une intervention liée à l'entretien des équipements. **Note :** La Commission d'accès à l'information exige la journalisation des numéros des dossiers consultés ou modifiés dans les banques de données médicales et médico-administratives.	Mesure 7.1
30. Le calendrier de conservation de la journalisation doit être établi en fonction des lois, normes et règlements en vigueur.	Mesure 7.5
Sécurité de l'exploitation des actifs informationnels	
• **Pour le service de l'exploitation informatique**	
31. Le calendrier des tâches assurées par le service de l'exploitation informatique quant à l'installation, à l'entretien et à la mise à jour de chaque logiciel et application doit être établi en fonction des besoins définis par le détenteur de l'actif informationnel.	
• **Pour le personnel du service de l'exploitation informatique**	
32. Le personnel affecté à l'exploitation des actifs informationnels ne doit pas accéder, sur une base continue, aux données de production. Une autorisation écrite par le détenteur de l'actif stipulera les circonstances lors desquelles l'accès et les modifications sont permis au personnel affecté à l'exploitation informatique ainsi que les contrôles que ce personnel pourra effectuer.	Mesure 2.3
33. L'utilisation des données de production à des fins de formation des utilisateurs est interdite sauf si l'autorisation du détenteur d'un actif ne contenant aucune information personnelle est accordée et que des mesures de contrôle supplémentaires sont mises en place.	Mesure 2.4
• **Pour la sauvegarde et la récupération des informations**	
34. Un plan de sauvegarde et de récupération des informations doit être élaboré et révisé périodiquement. Il précise, entre autres, la fréquence des copies de sécurité de toutes les informations (données, programmes informatiques, journaux d'accès), le lieu d'entreposage de ces copies, les personnes responsables de cette activité et les calendriers de conservation établis selon la classification des actifs.	Mesure 4.1

MESURES	EXIGENCES CAI[1]
35. Les copies de sécurité contenant des informations de nature hautement sensible sont conservées dans des locaux extérieurs au site d'origine de ces informations.	Mesure 4.4
36. Les copies de sécurité et les mécanismes de récupération des informations sont vérifiés régulièrement.	
37. La circulation des copies doit être contrôlée et l'accès aux copies de sécurité, restreint aux seules personnes autorisées.	Mesures 4.2 et 4.5
• **Pour la remise en état des systèmes**	
38. Un plan de reprise après sinistre (en cas de sinistre, de panne, d'intrusion, etc.) des systèmes en activité doit être mis par écrit et éprouvé régulièrement au moyen d'exercices de récupération des informations. Ce plan doit préciser, entre autres, le seuil de tolérance à l'interruption de chaque actif ainsi que les processus de relocalisation et les façons de revenir à la normale ; il doit également consigner l'historique des événements.	
39. Tous les documents à jour relatifs au plan de reprise après sinistre doivent être conservés à l'extérieur du site.	
• **Pour la gestion des mises à jour**	
40. Chaque organisme établit et applique des procédures et des mesures afin de continuer à assurer la sécurité des actifs informationnels pendant les changements apportés au système informatique.	
• **Pour la protection contre les attaques**	
41. Des mécanismes de protection contre les attaques (ex. : virus, intrusion, déni de service) internes et externes doivent être mis en place et tenus à jour afin de suivre l'évolution des menaces.	
42. Les accès non autorisés doivent être vérifiés. Des mesures préventives ou correctives doivent être appliquées pour les éviter.	Mesures 1.11 et 7.2
43. Un processus d'escalade en cas d'attaque doit être établi et éprouvé ; ce processus comprend notamment les actions permettant la reconstitution de la preuve.	
Sécurité des applications	
44. La sécurité doit être prise en compte dans les processus d'acquisition des logiciels et de développement des applications et au moment d'intégrer ces logiciels et applications à l'environnement technologique de l'organisme.	
45. Les logiciels et applications utilisés doivent être liés aux besoins d'affaires de l'organisme, être acquis légalement et respecter la Loi sur les droits d'auteur.	Mesure 13.2
46. Les logiciels et applications partageables entre les organismes par l'intermédiaire d'un réseau de télécommunications doivent être soumis à l'organisme mandaté par le MSSS pour en faire la certification.	
47. Les originaux des logiciels et des applications doivent être conservés sous clé et n'être accessibles qu'aux personnes autorisées.	
48. Une documentation structurée, claire et à jour concernant chaque logiciel et application informatique détenus par les organismes du RSSS doit être conservée dans un endroit sécuritaire.	
49. Les outils pour le soutien technique à distance (télédépannage et télédiagnostic) devront être préalablement homologués par le Bureau d'accueil et le Centre de certification avant d'être acquis et déployés.	

MESURES	EXIGENCES CAI[1]
Sécurité de l'impression	
50. L'impression d'informations confidentielles doit être limitée aux seules personnes autorisées par le détenteur de l'actif informationnel.	Mesure 14.1
51. Les applications doivent permettre la gestion des profils afin de limiter l'impression d'informations personnelles aux seules personnes autorisées.	Mesure 14.1
52. La clé « Print screen » et tous les outils de saisie d'image écran doivent être désactivés lorsque des informations nominatives apparaissent à l'écran afin d'empêcher l'impression non journalisée.	Mesure 13.3
53. Le détenteur détermine la localisation et le nombre d'imprimantes utilisables pour l'impression d'informations confidentielles contenues dans l'actif informationnel dont il a la responsabilité.	
Sécurité des télécommunications (réseaux locaux et étendus)	
54. Les organismes doivent respecter les exigences minimales de raccordement au Réseau de télécommunications sociosanitaire (RTSS).	
55. Les organismes doivent mettre en place une infrastructure réseau sécurisée intégrant les accès, les protocoles de communication, les systèmes d'exploitation et les équipements.	Mesure 13.2
56. Les organismes doivent sécuriser les données véhiculées par l'intermédiaire d'un réseau de télécommunications.	Mesure 8.2
57. Les organismes doivent faire évoluer les dispositifs de sécurité et les contrôles d'accès aux systèmes et aux données afin de contrer les nouvelles menaces et ils doivent vérifier périodiquement l'efficacité des mesures en place.	
58. La disponibilité des services locaux de télécommunications doit être assurée en fonction des besoins du détenteur de l'actif informationnel.	
REGISTRES DE SÉCURITÉ	
59. Les organismes du RSSS doivent élaborer et tenir à jour les trois registres de sécurité suivants : – le registre des autorités, contenant le nom des différents acteurs impliqués dans la gestion des actifs informationnels ainsi que leurs rôles et responsabilités ; – le registre des incidents, où sont consignés les événements ayant pu mettre en péril la sécurité des actifs informationnels ; – le registre des actes de gestion de la sécurité, contenant tout renseignement obtenu dans le cadre du processus de gestion de la sécurité ainsi que les documents, décisions ou directives rédigés par un acteur dans le cadre de ses fonctions en matière de sécurité.	
CONTRATS ET ENTENTES	
60. Les contrats et les ententes touchant les actifs informationnels, signés avec d'autres organismes du RSSS, avec des organismes externes ou avec des tiers, doivent préciser les exigences à respecter en matière de sécurité.	
61. Les contrats et ententes stipulent, entre autres, les points suivants : − le respect de la confidentialité ; − l'obligation de protéger les données, le mandataire étant responsable de l'application par son personnel de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels ; − les méthodes d'élimination des données stockées ;	Mesures 9.2 à 9.7

**Ceci est un extrait du guide CGGAI- volet sécurité, pages 60 à 64.*

Annexe 2 : Politique de sécurité des actifs informationnels

Agence de la santé
et des services sociaux
de Montréal
Québec

Politique de sécurité
des actifs informationnels

Le 30 août 2011

Version 1.6

POLITIQUE DE SÉCURITÉ - PROCESSUS DE VALIDATION

Politique type du CGGAI-volet sécurité	Le 22 mars au 10 mai 2006	Intégration des commentaires Agence incluant Carrefour montréalais, et deux sites TCR et DSP
Comité de sécurité des actifs informationnels	Le 10 mai 2006	Intégration des commentaires
Comité interdirection	Le 5 juin 2006	Intégration des commentaires
Comité de Planification et évaluation	Le 6 juin 2006	Recommandation au Conseil d'administration
Conseil d'administration	Le 20 juin 2006	Appuyé et résolu
Comité de sécurité des actifs informationnels (CSAI) - local	Le 21 janvier 2009	Intégration des commentaires du CSAI - local

REPRÉSENTANTS AU COMITÉ DE SÉCURITÉ DES ACTIFS INFORMATIONNELS (CSAI) - LOCAL

M. Frédéric Abergel	Directeur-adjoint, mission CHSGS
M. Ralès Bessard	Officier de la sécurité des actifs informationnels /RSAI
M. Serge Laniel	Responsable, services au réseau, Technologies et systèmes d'information, Technocentre régional
Mme Loraine Desjardins	Adjointe au directeur, Direction ressources humaines, information, planification et affaires et affaires juridiques
Mme Hélène Gendron	Chef de service, Systèmes d'information et de l'informatique
Mme Renée-Marthe Giard	Adjointe, secteur Administration, Direction de santé publique
Mme Sylvie Hubert	Chef de service, gestion de l'information
Mme Brigitte Lagacé	Commissaire régional aux plaintes et à la qualité des services
M. Vincent Lehouillier	Adjoint à la Direction Générale, Administration générale et ressources humaines
M. Roger Martin	Cadre-conseil, Direction gestion des immobilisations et des technologies médicales

Table des matières

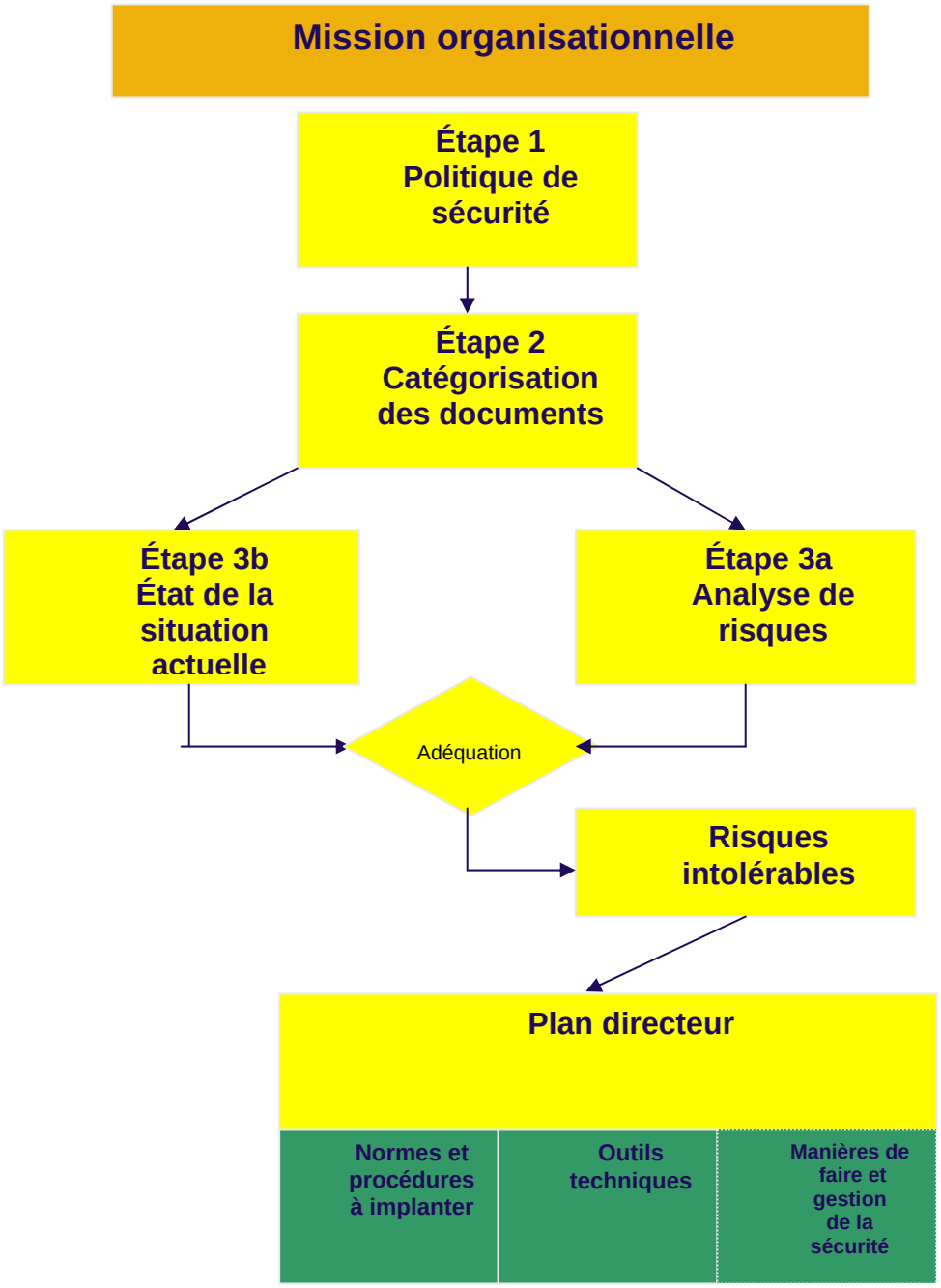
1. Contexte

La modernisation du réseau de la santé et des services sociaux repose sur la possibilité, pour les établissements et organismes du réseau, de s'échanger des informations de façon rapide et sécuritaire. C'est dans cette optique que le réseau s'est doté en 1999 du RTSS (réseau de télécommunication sociosanitaire) qui relie des sites au sein de plusieurs établissements et organismes de la santé. Dans la perspective d'un volume accru d'échanges d'information et afin de s'assurer du respect des lois, règlements et normes gouvernementales en matière de sécurité de l'information, le ministère de la Santé et des Services sociaux (MSSS) a élaboré et adopté le 22 septembre 2002 un Cadre global de gestion des actifs informationnels appartenant aux organismes de la santé et des services sociaux – volet sur la sécurité (CGGAI-volet sécurité). La volonté du MSSS est de mettre en place l'ensemble des mesures prévues au CGGAI-volet sécurité.

L'Agence reconnaît que l'information, sur support papier et électronique, est essentielle à ses opérations courantes et, de ce fait, qu'elle doit faire l'objet d'une évaluation, d'une utilisation appropriée et d'une protection adéquate. De plus, plusieurs lois et directives encadrent et régissent l'utilisation de l'information.

En conséquence, la présente politique de sécurité est la première de plusieurs étapes que l'Agence entreprend pour réaliser le plan de mise en œuvre du CGGAI-volet sécurité qui oriente et détermine l'utilisation appropriée et sécuritaire de l'information.

Étapes à venir pour réaliser le plan de mise en œuvre du CGGAI-volet sécurité :



2. Objectifs de la politique

La présente politique, vise à assurer le respect de toute législation à l'égard de l'usage et du traitement de l'information sur support **électronique et papier**, de l'utilisation des technologies de l'information et des télécommunications, ou autres manipulations de l'information.

Dans le présent document l'utilisation de l'expression « actif informationnel » signifie à la fois les documents sous format papier et les documents sous format électronique.

Fondés sur le CGGAI-volet sécurité, les objectifs de l'Agence de la santé et des services sociaux de Montréal sont d'assurer :

- la sécurité de l'information à l'égard de l'utilisation des actifs informationnels (a.i.) :
  - *objectifs de sécurité de l'information : disponibilité, intégrité, confidentialité;*
  - *objectifs de sécurité des accès et transmissions : authentification, irrévocabilité;*

- le respect de la vie privée de toute personne et des renseignements personnels relatifs aux utilisateurs et au personnel du réseau de la santé;

- le respect des mesures de sécurité et des différents codes de conduite concernant l'utilisation et la gestion des technologies de l'information et des télécommunications.

- la conformité aux lois et règlements applicables ainsi que les directives, normes et orientations gouvernementales.

Cette politique sera suivie de normes et de procédures afin de préciser les obligations qui en découlent.

3. Portée

La portée de la présente politique s'applique à toute personne physique ou morale qui utilise ou accède à de l'information, quelque soit le support sur lequel elle est conservée.

La portée comporte deux dimensions :

3.1. Les personnes visées

- tout le personnel de l'Agence, incluant le personnel du Carrefour montréalais de l'information sociosanitaire et le personnel des deux autres sites soit celui du Technocentre de Montréal et celui de la Direction de la Santé publique*;

(*ces derniers, par leur vocation particulière, peuvent ajouter des procédures reliées à leurs activités spéciales selon un processus de validation tant et aussi longtemps qu'ils sont conformes à la présente politique de l'Agence);
- tous les fournisseurs, contractuels, chercheurs, stagiaires et entités externes qui doivent accéder à notre réseau.

3.2. Les actifs et services visés

- l'ensemble des actifs informationnels appartenant ou sous la responsabilité de l'Agence ainsi que leur utilisation au sein de celle-ci;
- les contrats et les ententes de services en lien avec des actifs informationnels;
- toute information traitée électroniquement et/ou conservée sur papier.

4. Respect de la politique

Le président-directeur général de l'Agence désigne l'Officier de sécurité de l'information/Responsable de la sécurité des actifs informationnels (RSAI) comme responsable de l'application de la présente politique.

L'Agence exige de toutes les personnes qui utilisent les actifs informationnels ou qui ont accès à de l'information de se conformer aux dispositions de la présente politique ainsi qu'aux normes, directives et procédures qui s'y rattachent.

Le non-respect de cette obligation peut entraîner des mesures disciplinaires pouvant aller jusqu'au congédiement immédiat selon la nature de la faute.

5. Principes, éléments et normes de la politique

La présente politique de sécurité origine de l'obligation de se conformer au CGGAI-volet sécurité en vue de protéger les 7 principaux domaines à considérer dans une approche globale de gestion de l'information. Ils déterminent les grands paramètres de la sécurité de l'information dans le réseau de la santé et des services sociaux orientant notre politique locale. Ces principaux domaines sont les suivants :

- lois en vigueur dans le domaine de la santé et des services sociaux, lois et règlements internationaux, canadiens et québécois;
- protection de la vie privée;
- protection des renseignements personnels;
- accès à l'information;
- gestion des documents et des archives (quel que soit le support);
- propriété intellectuelle;
- protection des données corporatives.

Chaque domaine de gestion de l'information génère des obligations en regard des objectifs de sécurité de l'information, d'accès et de transmission des données. Le schéma sur le positionnement de la sécurité de l'information du Réseau de la santé et des services sociaux (RSSS) situe bien notre politique de sécurité locale (voir annexe 3).

5.1. Principes directeurs

a. Toute personne ayant accès aux actifs informationnels assume des responsabilités spécifiques en matière de sécurité et est imputable de ses actions auprès de son supérieur immédiat. Elle applique et respecte la politique de sécurité et ses normes et procédures ainsi que les lois et règlements spécifiques à son domaine d'activité. Elle avise son supérieur immédiat de toute situation susceptible de compromettre la sécurité des actifs informationnels.

b. La mise en œuvre et la gestion de la sécurité reposent sur une approche globale et intégrée. Cette approche tient compte des aspects humains, organisationnels, financiers, juridiques et techniques, et demande, à cet égard, la mise en place d'un ensemble de mesures coordonnées.

c. Les mesures de protection, de prévention, de détection, d'assurance et de correction doivent permettre d'assurer la disponibilité, l'intégrité et la confidentialité, l'authentification et l'irrévocabilité des actifs informationnels de même que la continuité des activités. Elles doivent notamment empêcher les accidents, les erreurs, la malveillance ou la destruction d'information sans autorisation.

d. Les mesures de protection des actifs informationnels doivent permettre de respecter les prescriptions du CGGAI-volet sécurité de même que les lois existantes en matière de conservation, d'accès, de diffusion et de transmission d'information, les obligations contractuelles de l'Agence et l'application des règles de gestion interne. Ces mesures permettent aussi de gérer adéquatement l'utilisation d'Internet, d'intranet, du courrier électronique, du réseau interne de l'Agence et du RTSS.

e. Afin de reconnaître toute information sensible, **tout actif informationnel** doit faire l'objet d'une identification et d'une catégorisation selon un processus continu d'évaluation de l'information.

f. Une évaluation périodique des risques et des mesures de protection des actifs informationnels doit être effectuée afin d'obtenir l'assurance qu'il y a adéquation entre les risques, les menaces et les mesures de protection déployées.

g. La gestion de la sécurité de l'information doit être incluse et appliquée tout au long du processus menant à l'acquisition, au développement, à l'utilisation, au remplacement ou la destruction d'un actif informationnel par ou pour l'Agence.

h. Un programme continu de sensibilisation et de formation à la sécurité de l'information doit être mis en place.

i. Tous les actifs informationnels sont dédiés et réservés à la réalisation des activités de l'Agence. Cependant, en tenant compte que le travail a la priorité, l'Agence reconnaît que les utilisateurs peuvent, en lien avec la loi et en dehors des heures de travail, utiliser son réseau à des fins personnelles, tout

en s'assurant que la présente politique est respectée en tous points. En aucun cas, l'Agence ne peut être tenue responsable envers l'utilisateur de tout dommage, perte ou conséquence découlant d'une interruption volontaire ou d'une panne de son réseau ou d'en faire une utilisation inappropriée.

j. Les renseignements personnels, confidentiels et nominatifs ne doivent être utilisés qu'aux fins pour lesquelles ils ont été recueillis ou obtenus. Ils ne doivent pas être divulgués, sauf si leur communication est autorisée par une loi ou un règlement.

k. Le principe du « droit d'accès minimal » est appliqué en tout temps lors de l'attribution d'accès aux informations. Les accès aux actifs informationnels sont attribués à l'utilisateur autorisé en fonction de ce qui lui est strictement nécessaire pour l'exécution de ses tâches.

l. L'utilisation des actifs informationnels de l'Agence est un privilège. Ce privilège peut être révoqué, en tout temps, à tout utilisateur qui se servira de manière inappropriée des actifs informationnels mis à sa disposition et qui ne se conformera pas à la politique. Tout usage dérogatoire des actifs informationnels est sanctionné selon toute source conventionnelle, légale ou réglementaire à la disposition de l'Agence.

m. Les ententes et contrats en lien avec les actifs informationnels doivent contenir des dispositions garantissant le respect des exigences en matière de sécurité et de protection de l'information.

5.2. Éléments et normes de la politique[1]

Le CGGAI-volet sécurité vise la protection de tous les actifs informationnels définis selon huit (8) catégories tirées du CGGAI-volet sécurité (voir annexe 4) :

1. Organisation et administration de la sécurité

L'Agence doit assurer une gestion de la sécurité des actifs informationnels. Elle doit établir un programme de sensibilisation et de formation dans le but de faciliter l'application des mesures de sécurité informatique et la responsabilisation des individus face aux actes posés en regard de la sécurité de l'information et aux conséquences de leurs actions. Elle doit déterminer des niveaux de risque acceptables et évaluer les menaces touchant les actifs informationnels. Elle doit avoir un processus d'inventaire et de catégorisation de ses actifs informationnels lui permettant d'établir un niveau de protection adéquat et d'assurer la continuité des opérations.

2. Sécurité logique, gestion des accès et utilisation

L'Agence doit assurer la sécurité des actifs informationnels par un processus formel de gestion et de contrôle des codes et profils d'accès accordés à ses utilisateurs et définir les mesures de gestion et d'utilisation sécuritaire des mots

[1] Cette section est largement inspirée de la politique en vigueur à l'hôpital Louis-H Lafontaine.

de passe. Elle doit assurer la présence de contrôles adéquats (journalisation) pour détecter, vérifier et valider les accès aux systèmes et le respect des mesures et procédures de sécurité de l'Agence.

3. Sécurité physique, prévention, détection et protection

L'Agence doit définir les mesures nécessaires afin de prévenir les accès non autorisés aux actifs informationnels incluant les accès aux classeurs, aux espaces de travail et d'entreposage. Elle doit assurer la mise en place d'un processus efficace d'accès, de gestion et de contrôle de ses classeurs, de son matériel informatique et de télécommunication et autres installations.

4. Développement, maintenance et mise en place des systèmes

L'Agence doit assurer la prise en compte des considérations liées à la sécurité lors du développement, de l'acquisition, de l'entretien et de la mise en place de tout système informatique. Elle doit assurer la mise en place d'un processus de gestion des changements garantissant la sécurité et l'intégrité des systèmes d'application et des données. Elle doit aussi assurer la gestion adéquate des contrats et ententes touchant les actifs informationnels. Ces derniers doivent contenir des dispositions garantissant le respect des exigences en matière de sécurité et de protection de l'information selon l'encadrement du CGGAI-volet sécurité.

5. Exploitation informatique

L'Agence doit assurer la présence de directives adéquates reliées à l'exécution des opérations informatiques et à leurs résultats. Personne ne peut altérer (modifier, ajouter ou corriger) de quelque façon que ce soit les données de production ou entreprendre des travaux de son propre chef sans autorisation écrite du détenteur de l'actif informationnel. L'Agence définit aussi les règles à suivre face aux antivirus et à l'application des mesures antivirus. Elle doit assurer la gestion et l'utilisation sécuritaire de la fonction d'impression et définir des mesures nécessaires pour garantir la sécurité des réseaux de télécommunication. Elle doit aussi définir les bases d'un processus local de réponse et d'escalade en cas d'attaque, tant interne qu'externe. La définition d'attaque inclut, entre autres, le «hacking», les dénis de service, les virus et l'utilisation inappropriée des actifs informationnels.

6. Réseautique

Les utilisateurs ont accès au réseau Internet, au RTSS et au réseau interne mis en place par l'Agence, incluant les utilisateurs effectuant des activités de recherche et d'évaluation. Chaque utilisateur du réseau de télécommunication doit pouvoir être identifié de façon unique et doit authentifier son identité pour accéder au réseau de façon à exercer l'imputabilité. Ce qui signifie qu'un

utilisateur ne peut en aucun cas utiliser le compte d'un autre utilisateur pour accéder au réseau.

Les règles et les mesures de sécurité entourant les réseaux de télécommunication et d'Internet doivent empêcher quiconque d'intercepter des données sensibles sans autorisation. De plus, elles doivent assurer la continuité des opérations et l'intégrité dans la transmission des données.

7. Micro-informatique

L'Agence doit assurer l'installation de logiciels et de progiciels autorisés pour lesquels des licences valides existent sur les serveurs et les postes de travail des utilisateurs afin d'éviter les conséquences légales liées au non-respect des droits d'auteur. Aucun logiciel ne peut être installé par un utilisateur sans autorisation préalable.

Tout document électronique de source externe doit être vérifié contre les virus avant son exécution ou son utilisation. S'il y a présence de virus ou un doute raisonnable qu'il y en a un, il est formellement interdit d'utiliser ce document dans les appareils de l'Agence ou sur son réseau.

Les données sensibles ne doivent pas être emmagasinées sur les postes de travail sans raison valable. En cas de besoin, elles doivent être protégées de façon sécuritaire (exemple : chiffrement, mot de passe, etc).

8. Relève en cas de désastre ou de panne

L'Agence doit définir les mesures nécessaires afin d'assurer la continuité et la reprise rapide des opérations en cas de non-disponibilité de ses systèmes informatiques pour une période intolérable.

Elle doit assurer la mise en place d'un mécanisme de protection de ses données critiques contre la corruption ou la perte suite à une défaillance technique, une suppression ou une modification involontaire ou malveillante. Le mécanisme contribuera au succès d'une opération de relève en cas de désastre en assurant la disponibilité et l'intégrité de ses données.

6. Définition des termes spécifiques utilisés

Voir Annexe 2.

7. Rôles et responsabilités au sein de l'agence

Cette section vise à établir les rôles et responsabilités de chacun selon les fonctions qu'il occupe au sein de l'Agence.

- **Le conseil d'administration de l'Agence**
  - doit approuver la présente politique;
  - reçoit le bilan annuel résultant de l'application de la politique.

- **Le président-directeur général**
  Le président-directeur général est le premier responsable de la sécurité des actifs informationnels.
  - nomme le responsable de la sécurité des actifs informationnels (RSAI);
  - voit à ce que les valeurs et les orientations en matière de sécurité soient partagées par l'ensemble des gestionnaires et du personnel;
  - s'assure de sa mise en œuvre et fait le suivi de son application;
  - soumet le bilan annuel résultant de l'application de la politique au conseil d'administration.

- **Le comité de sécurité des actifs informationnels (CSAI) - local**
  Le comité de sécurité des actifs informationnels local est un comité permanent:
  - a un rôle de conseil auprès du RSAI;
  - assure l'application des différentes mesures de sécurité identifiées dans le CGGAI–volet sécurité, soutient la mise en place des dispositions législatives et propose 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;
  - évalue les incidences sur la sécurité de l'organisation que les nouveaux projets pourraient avoir;
  - constitue un mécanisme de coordination et de concertation qui, par sa vision globale, est en mesure de proposer des orientations et de faire des recommandations au 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;
  - effectue le suivi de l'échéancier et rend des comptes au PDG.

- **Le responsable de la sécurité des actifs informationnels (RSAI)**
  À titre de représentant délégué du président-directeur général en matière de sécurité des actifs informationnels, il gère et coordonne la sécurité au sein de l'Agence :
  - harmonise l'action des divers acteurs dans l'élaboration, la mise en place, le suivi et l'évaluation de la sécurité de l'information;
  - coordonne les activités reliées au CGGAI-volet sécurité;
  - veille à l'élaboration et à l'application de la politique sur la sécurité;
  - établit un programme général d'application et de respect de la présente politique;
  - gère les aspects relatifs à l'escalade des incidents de sécurité;
  - suit la mise en œuvre de toute recommandation découlant d'une vérification ou d'un audit;
  - produit annuellement, et au besoin, des rapports relatifs à la sécurité de l'information.

- **Analyste en sécurité**

  À titre d'analyste en sécurité:
  - travaille sous la gestion professionnelle du RSAI;
  - s'assure d'être au courant du CGGAI-volet sécurité;
  - met en place des procédures pour appuyer l'implantation des mesures obligatoires du CGGAI-volet sécurité en collaboration avec le service des systèmes d'information et de l'informatique de l'Agence;
  - coordonne et/ou réalise les tâches de sécurité opérationnelles qui lui sont confiées par le RSAI;
  - informe le RSAI de tout manquement à la politique.

- **Les services des systèmes d'information et de l'informatique**

  Le service des systèmes d'information et de l'informatique agit comme fournisseur des services suivants sans s'y limiter :
  - fournit et maintient en état les moyens techniques de sécurité dans l'exploitation des actifs informationnels;
  - assure la conformité de ces moyens techniques en fonction des besoins de sécurité déterminés par le détenteur d'actif;
  - assiste et conseille les utilisateurs en vue d'une meilleure utilisation de ces moyens techniques;
  - met en application la politique de compte d'usagers, les procédures des profils et des codes d'accès;
  - voit à la tenue des inventaires sur les équipements et logiciels;
  - voit à la gestion des mots de passe;
  - voit à la mise en place des antivirus et à la tenue des journaux;
  - assure la sécurité dans le développement d'applications informatiques;
  - met en place et maintient une relève des actifs informationnels classés prioritaires;
  - conseille les directeurs de l'Agence dans l'acquisition des équipements, des logiciels et du matériel nécessaires pour appliquer la présente politique;
  - voit 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;
  - appuie le RSAI dans son rôle.

- **Le gestionnaire**
  - en lien avec les sessions de sensibilisation à la sécurité, le gestionnaire s'assure que son personnel est au fait de leurs obligations découlant de la présente politique, normes et procédures de sécurité en vigueur;
  - s'assure que des moyens de sécurité sont utilisés de façon à protéger l'information utilisée par son personnel;
  - demande les droits d'accès aux applications pour son personnel dans le cas où il n'est pas détenteur;
  - informe le RSAI de toute situation à risque dans le but d'améliorer la sécurité des a.i.. Les critères pour un incident sont :
    - Impacts sur la prestation des services aux usagers;
    - Impacts légaux;
    - Impacts sur plus d'un établissement ou organisme;
    - Tout évènement pouvant compromettre la sécurité physique, la sécurité logique, la sécurité de l'impression, etc.;
  - voit au suivi des codes de conduite émis par le service des ressources humaines.

- **Le détenteur d'actifs informationnels**
  - participe à l'ensemble des activités relatives à la sécurité, notamment l'évaluation des risques, la détermination du niveau de protection visé, l'élaboration des contrôles non informatiques, la prise en charge des risques résiduels concernant les actifs informationnels et, finalement;
    - autorise les droits d'accès aux informations incluant les systèmes d'information dont il est détenteur;
    - assure la sécurité d'un ou de plusieurs actifs informationnels;
    - s'assure que les mesures de sécurité appropriées sont élaborées, approuvées, mises en place et appliquées systématiquement en plus de s'assurer que leur nom et les actifs dont ils assument la responsabilité sont consignés dans le registre des autorités (formulaire d'autorisation des accès).

- **Pilote de système nommé par le détenteur de l'actif informationnel**
  - assure le fonctionnement sécuritaire d'un actif informationnel dès sa mise en exploitation;
  - contrôle et donne l'accès à l'actif informationnel dont il a la responsabilité à la demande du détenteur de l'actif et en collaboration avec le service des systèmes d'information et de l'informatique;
  - informe les utilisateurs de leurs obligations face à l'utilisation des systèmes d'information lors de l'attribution des accès.

- **Responsable de la protection des renseignements personnels (RPRP)** - À titre de responsable de l'application de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, le RPRP a un rôle de conseiller et/ou de valideur - approbateur auprès du RSAI afin de :
  - s'assurer que les mécanismes de sécurité mis en place permettent de respecter les exigences de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels;
  - de voir à ce que cette responsabilité se manifeste dès le début d'un développement d'un nouveau système où le RPRP doit introduire les préoccupations et les exigences relatives à la protection des renseignements nominatifs.

- **Service interne des ressources humaines**
  - est responsable d'informer toute nouvelle personne de ses obligations découlant de la présente politique;
  - est responsable de sensibiliser toute nouvelle personne aux enjeux reliés à la sécurité des actifs informationnels**;**
  - est responsable de voir à la signature de l'engagement au secret professionnel et à la confidentialité des données.

- **L'utilisateur**
  - prend connaissance de la politique de sécurité;
  - respecte la présente politique, normes, directives et procédures en vigueur en matière de sécurité de l'information;
  - si applicable, signe le(s) formulaire(s) d'engagement selon le(s) service(s) utilisé(s) (i.e. engagement au secret professionnel et à la confidentialité des données, politique d'utilisation d'internet et courrier électronique, etc.);

- avise le supérieur hiérarchique dès qu'il constate un manquement à la politique.

8. Mise en application

Des normes et des procédures découlent de la présente politique.

Dans tous les cas elles sont mises à jour afin de tenir compte des développements législatifs, technologiques ou de l'évolution dans les modes d'utilisation.

Le CMIS ainsi que les deux sites soit celui du Technocentre de Montréal et celui de la Direction de la Santé publique, par leur vocation particulière, doivent respecter les exigences de la présente politique mais peuvent développer et ajouter des procédures reliées à leur activités spéciales selon un processus de validation.

Les annexes font partie intégrante de la politique.

9. Mises à jour

La révision de la présente politique sera faite selon un calendrier établi par le CSAI.

ANNEXE 1

RÉFÉRENCES

1. Charte des droits et libertés de la personne, (L.R.Q. c. C-12)

2. Loi sur les services de santé et services sociaux, Québec, (L.R.Q., c.A-4.2)

3. Loi 83, Loi modifiant la Loi sur les Services de santé et les Services sociaux et d'autres dispositions législatives

4. Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, Québec, (L.R.Q. c. a-2.1)

5. Exigences minimales relatives à la sécurité des dossiers informatisés des usagers du réseau de la santé et des services sociaux, Commission d'Accès à l'Information du Québec, Québec, 1992

6. Politique intérimaire de sécurité visant les actifs informationnels du réseau de la santé et des services sociaux, RTSS, Québec, 1999

7. Politique administrative relative à la sécurité des actifs informationnels et de télécommunication et à la protection des données et des renseignements confidentiels de la Régie régionale de la santé et des services sociaux de Québec, RRSSS de Québec, Québec, 2000

8. Le cadre global de gestion des actifs informationnels du réseau de la santé et des services sociaux, septembre 2002

9. Le courrier électronique, Commission d'accès à l'information du Québec, Québec, 1997

10. Loi sur les droits d'auteur, (L.R.C., c.C.42)

11. Loi sur les Archives, (L.R.Q., c.A-21.1)

12. MSSSQ, projet de standard, version 1.1, juin 2003, annexe A - Exemple de politique

ANNEXE 2

DÉFINITION DES TERMES UTILISÉS

Actif informationnel (a.i.)

Système d'information, matériel informatique et de télécommunication, logiciels, progiciels, banques de données et information (textuelle, sonore, symbolique ou visuelle) placées dans un matériel informatique ou sur un média informatique et/ou électronique, système de courrier électronique. Un équipement médical spécialisé ou ultraspécialisé 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 papiers et les documents imprimés générés par les technologies de l'information.

Cadre global de gestion des actifs informationnels appartenant aux organismes du réseau de la santé et des services sociaux – Volet sur la sécurité (CGGAI-volet sécurité)

Ensemble de textes encadrant la sécurité des actifs informationnels et comprenant la Politique nationale sur la sécurité des a.i., les rôles et responsabilités des acteurs en matière de sécurité, les mesures en matière de sécurité des a.i. et le répertoire des procédures optionnelles en cette matière.

Code de conduite

Condensé de règles de pratique élaborées à partir de principes éthiques moraux et professionnels, devoirs et responsabilités, destiné à établir des règles de conduite à suivre et régissant particulièrement l'utilisation des actifs informationnels ainsi que la protection des données et des renseignements confidentiels.

Données sensibles

Toute information pouvant créer préjudice à l'Agence ou à toute autre personne.

Incident

Événement ayant mis en péril la sécurité d'un ou de plusieurs actifs informationnels.
Les critères pour un incident sont : Impacts sur la prestation de services aux usagers; Impacts légaux; Impacts sur plus d'un établissement ou site; Tout événement pouvant compromettre la sécurité physique, la sécurité logique, la sécurité de l'impression, etc.

Exemple d'incidents potentiels dus à des:

- *menaces … intrusions, détection de virus;*
- *risques … modifications de l'environnement technologique comme le raccordement au RTSS ou le déploiement de nouvelles applications.*

Information

Élément de connaissance descriptif d'une situation ou d'un fait, résultant de plusieurs données.

Information électronique

Information sous toute forme (textuelle, symbolique, sonore ou visuelle), dont l'accès et l'utilisation ne sont possibles qu'au moyen des technologies de l'information.

Intranet ou réseau Intranet

Réseau informatique privé de l'Agence qui utilise des protocoles de communication et des technologies permettant un échange interne d'information. Les protocoles et les technologies les plus connus sont ceux d'Internet.

Journalisation

Enregistrement dans un journal de tous les accès fructueux et infructueux à un ordinateur et aux données, de l'utilisation de certains privilèges spéciaux relatifs à l'accès et des changements apportés aux a.i., en vue d'une vérification ultérieure.

Mot de passe

Authentifiant prenant la forme d'un code alphanumérique attribué à un utilisateur (code d'accès, «d'usager»), permettant à ce dernier d'obtenir l'accès à un ordinateur en ligne et d'y effectuer l'opération désirée. Cet authentifiant représente une liste secrète de caractères qui, combinée à un code d'utilisateur public, forme un identificateur unique désignant un utilisateur particulier.

Normes et pratiques

Énoncés généraux émanant de la direction de l'Agence et indiquant ce qui doit être appliqué relativement à la sécurité des actifs informationnels.

Renseignements nominatifs

Sont nominatifs les renseignements qui concernent une personne physique et permettent de l'identifier. Le nom d'une personne physique n'est pas, en soi, un renseignement nominatif, sauf lorsqu'il est mentionné avec un autre renseignement la concernant ou lorsque sa seule mention révélerait un renseignement nominatif concernant cette personne.

RTSS (Réseau de télécommunications sociosanitaire)

C'est le principal véhicule d'échange électronique d'information entre les établissements et organismes du réseau de la santé et des services sociaux.

RSSS

Réseau de la santé et des services sociaux.

Sécurité de l'information

La prémisse sur laquelle se base la sécurité de l'information s'articule autour de 5 fonctions dont l'acronyme est DICAI.

Trois fonctions de sécurité de l'information (1 à 3) et deux fonctions de sécurité des transmissions de l'information (4-5) :

1. Disponibilité : propriété d'une information d'être accessible et utilisable en temps voulu et de la manière requise par une personne autorisée;
2. Intégrité : propriété d'une information ou d'une technologie de l'information de n'être ni modifiée, ni altérée, ni détruite sans autorisation;
3. Confidentialité : propriété d'une information d'être inaccessible aux personnes non autorisées;
4. Authentification : acte permettant d'établir la validité de l'identité d'une personne ou d'un dispositif;

5. Irrévocabilité : propriété d'un acte d'être définitif et qui est clairement attribué à la personne qui l'a posé ou au dispositif avec lequel cet acte a été accompli.

Donc assurer la disponibilité, l'intégrité, la confidentialité, l'authentification et l'irrévocabilité des actifs informationnels et la continuité des activités en regard des réseaux informatiques, du RTSS, d'Internet et d'intranet et des données organisationnelles sur support informatique.

Systèmes d'information

Ensemble des pratiques et des moyens pour recueillir, traiter, mettre à jour, reproduire et distribuer tous les types d'informations en vue de répondre à un besoin déterminé y incluant notamment les TI et les procédés utilisés pour accomplir ces fonctions.

Technologie de l'information (TI)

Tout logiciel ou matériel électronique et toute combinaison de ces éléments utilisés pour recueillir, emmagasiner, traiter, communiquer, protéger ou éliminer l'information sous toute forme (textuelle, symbolique, sonore ou visuelle).

Toute nouvelle personne

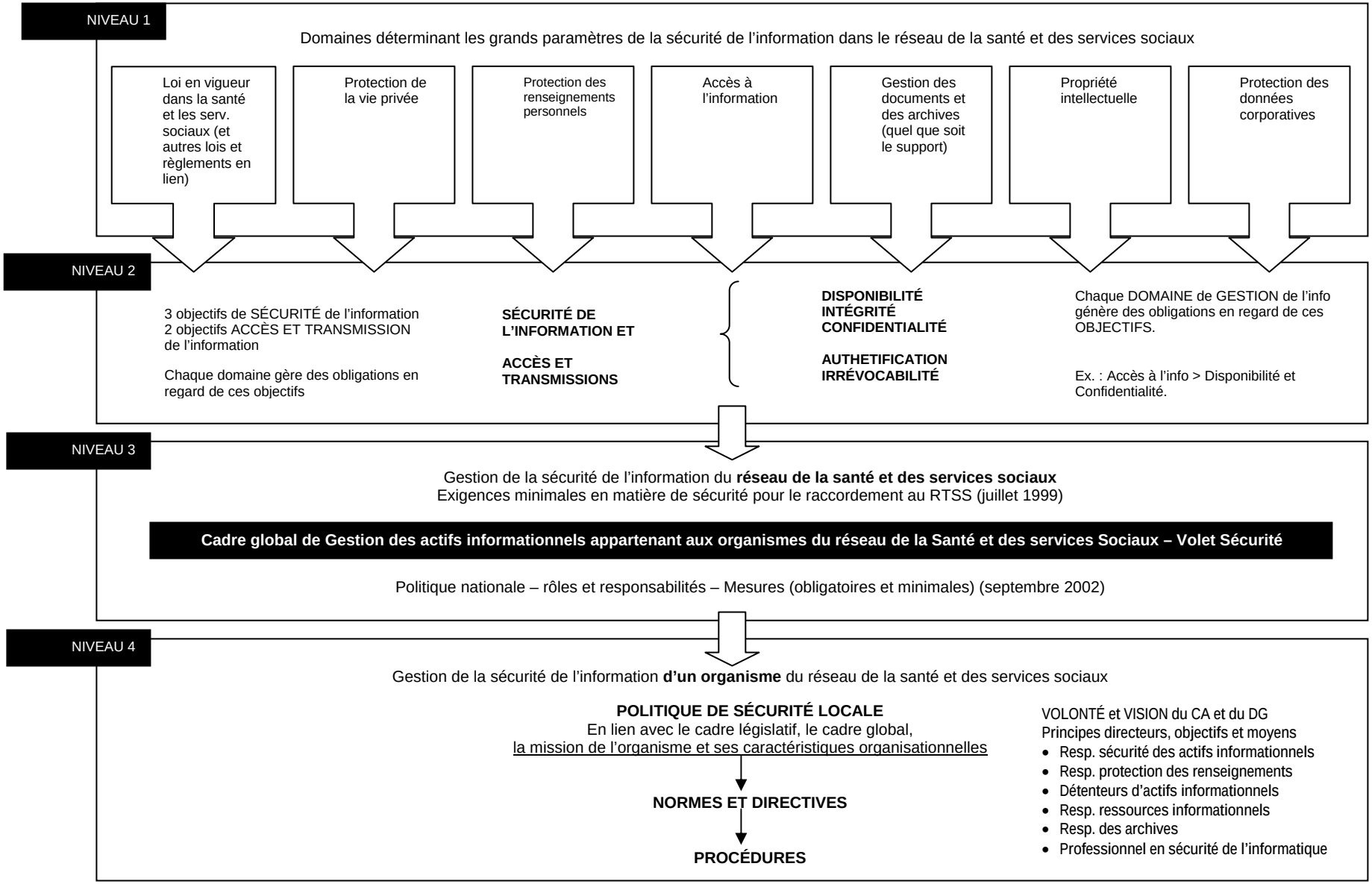
Tout nouvel employé permanent ou temporaire à temps plein ou à temps partiel, tout nouveau contractuel, consultant, chercheur, stagiaire, fournisseur et entités externes qui travaillent pour l'Agence incluant la santé publique, le Technocentre de Montréal et le CMIS ou toute nouvelle personne qui travaille pour le compte d'une entité externe mais dans les locaux de l'Agence, incluant les locaux de la santé publique, ceux du CMIS et ceux du Technocentre.

Annexe 3

POSITIONNEMENT de la SÉCURITÉ DE L'INFORMATION du RÉSEAU de la SANTÉ et des SERVICES SOCIAUX

Chaque niveau influence le suivant

(Adapté du GUIDE DE RÉDACTION, juin 2003, version 1.1)

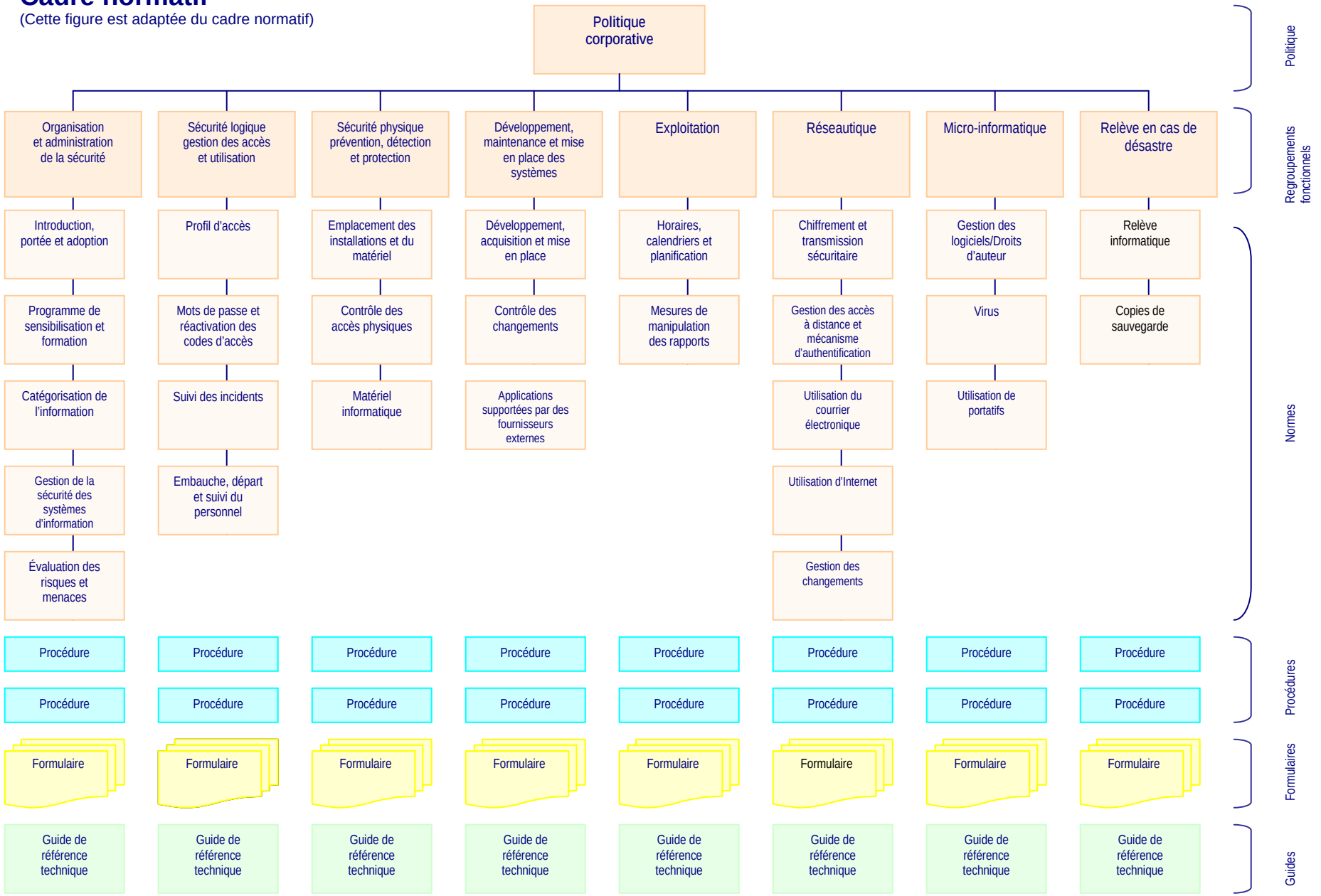


Annexe 4

Éléments et normes de la politique

Cadre normatif

(Cette figure est adaptée du cadre normatif)



Annexe 3 : Plan directeur de la sécurité

Agence de la santé
et des services sociaux
de Montréal
Québec

Plan directeur de la sécurité de l'information (2009-2012)

Version : 1.7 **Mise à jour du document :** 6 avril 2009 **DIC :** 1.2.2

Historique du document

Version	Description	Auteur	Date
1.0	▪ Élaboration du document « Plan directeur de la sécurité de l'information »	Comité de travail	2008-08-20
1.1	▪ Intégration de la notion de ressources internes et externes	CSAI	2008-10-10
1.2	▪ Ajout d'un tableau sommaire des coûts pour les 3 sites ▪ Ajout des coûts relatifs au suivi et à la coordination de la mise en œuvre du plan directeur pour chacun des 3 sites	Comité de travail	2008-12-06
1.3	▪ Modification du taux horaire pour les professionnels de la sécurité (40 $/h au lieu de 60 $/h) dans les 3 plans directeurs	CSAI	2009-01-26
1.4	▪ Ajout de la colonne "Ressources sollicitées" dans les 3 plans directeurs	Comité de travail	2009-02-03
1.5	▪ Ajout du ratio de sollicitation (70 % l'année 1, 50 % l'année 2 et t 50 % l'année 3) pour les coordonnateurs de la mise en œuvre des plans directeurs ▪ Ajout des colonnes (efforts et coûts absorbés dans les coûts non récurrents : cela fait ressortir la portion des coûts absorbés par chacun des sites	Comité de travail	2009-03-12
1.6	▪ Révision et modifications	Lisette Martin	2009-03-26
1.7	▪ Approbation	CSAI	2009-04-06

Représentants au sous comité de sécurité des actifs informationnels (CSAI) local / Comité de travail

Mme Louise Francoeur	Analyste en informatique à la Direction de santé publique
Mme Hélène Gendron	Chef de service, Systèmes d'information et de l'informatique
Mme Renée-Marthe Giard	Chef du service informatique et du service des finances de la Direction de santé publique
M. Mario L'Écuyer	Chef de l'exploitation, Technocentre régional
M. Imad Znini	Officier de la sécurité des actifs informationnels

Représentants au comité de sécurité des actifs informationnels (CSAI) local

M. Diamantino De Sousa	Coordonnateur, Technologies et systèmes d'information
Mme Hélène Gendron	Chef de service, Systèmes d'information et de l'informatique
Mme Renée-Marthe Giard	Chef du service informatique et du service des finances de la Direction de santé publique
M. Jocelyn Lavallée	Coordonnateur par intérim, gestion de l'information
M. Roger Martin	Cadre-conseil, Direction associée gestion des immobilisations et des technologies médicales
Mme Ghislaine Tremblay	Commissaire régional aux plaintes et à la qualité des services
M. Gérald Trottier	Adjoint à la DGA, Administration générale et ressources humaines
Mme Carolle Turcotte	Directrice associée, Ressources humaines, relation avec la population et affaires juridiques
M. Imad Znini	Officier de la sécurité des actifs informationnels /RSAI

Table des matières

1. INTRODUCTION

1.1. MISE EN CONTEXTE

La sécurité des actifs informationnels est devenue une préoccupation majeure des intervenants œuvrant dans le domaine de la santé. Il est facile de comprendre les enjeux reliés à la sécurisation des actifs informationnels étant donné l'importance stratégique des systèmes d'information utilisés par les organismes de même que la nature sensible des informations qu'ils traitent.

En ce sens, 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. Le Cadre global vise à communiquer les attentes, les obligations et les rôles de chacun des intervenants en matière de sécurité des actifs informationnels. Le ministère a aussi élaboré un document portant sur la protection des renseignements personnels. Ce document s'intitule « **Cadre global de gestion des actifs informationnels appartenant aux établissements du réseau de la santé et des services sociaux – Volet sur la protection des renseignements personnels »** et dénote l'inclusion de la dimension « protection des renseignements personnels » dans l'approche de sécurité.

C'est donc dans ce contexte que la catégorisation des actifs informationnels ainsi que l'analyse des risques ont été réalisées à l'Agence, afin de produire, ultimement, un plan d'actions triennal en établissant les priorités d'amélioration selon les conclusions tirées des deux phases précédentes. Ce plan d'action se dénomme le *Plan directeur de la sécurité de l'information.*

1.2. RAISON D'ÊTRE DU DOCUMENT

Le plan directeur de la sécurité de l'information (plan directeur) constitue le document officiel pour la mise en œuvre du Cadre global de la gestion de la sécurité des actifs informationnels – volet sécurité, sur un horizon temporel de 3 ans. Il énumère les actions et les contrôles que l'Agence devra entreprendre et implanter afin de mitiger les risques inhérents à la sécurité des ses actifs informationnels. Ce plan regroupe autant les actions de type stratégique que de type opérationnel.

1.3. PORTÉE DU PLAN DIRECTEUR

Le plan directeur englobe l'Agence et ses deux sites, soit celui du Technocentre régional et celui de la Direction de santé publique.

1.4. PRÉMISSES

1) Le plan directeur de la sécurité se base sur des analyses de risques effectuées sur les actifs informationnels de l'Agence et de ses sites : siège social (3725 St-Denis), Technocentre régional et Direction de santé publique.

2) Étant donné que les sites de l'Agence ont des contextes et des réalités technologiques différents, chacun de ces sites aura son propre plan directeur.

3) Les plans directeurs sont triennaux et doivent être approuvés par le conseil d'administration de l'Agence (conformément à la politique de la sécurité et aux exigences du MSSS).

4) Les dépenses absorbées par l'Agence (site St-Denis et DSP) seront soustraites uniquement des coûts non récurrents du plan directeur (3 ans) étant donné qu'il n'y a pas d'enveloppe budgétaire récurrente pour la sécurité. Ses ressources internes étant sollicitées à 100 %, le Technocentre ne pourrait absorber de coûts.

5) Les ressources internes concernent les personnes (déjà employées ou à embaucher) gérées par l'Agence. Les ressources externes sont des personnes externes embauchées par l'Agence (donc ne faisant pas partie de celle-ci) soit par manque d'expertise ou de capacité.

6) La mise en œuvre des actions du plan (dans leur intégralité ou en partie) dépendra des ressources qui seront octroyées par la haute direction.

7) La planification de la mise en œuvre du plan directeur commencera immédiatement après l'approbation du conseil d'administration de l'Agence.

8) Étant donné qu'il est impossible de tout protéger, les actions des plans directeurs ont été priorisées selon les niveaux de risque auxquels sont exposés les actifs informationnels.

9) Par souci d'optimisation et de rationalisation de dépenses, le comité de travail a retenu (parmi plusieurs scénarios) le scénario de coûts engendrant le moins de dépenses pour l'Agence sans que cela ne biaise la priorisation des actions des plans directeurs.

2. COÛTS DES PLANS DIRECTEURS

2.1. SOMMAIRE DES COÛTS

Les tableaux, ci-après, représentent les coûts (récurrents et non récurrents) des plans directeurs des 3 sites. Ces coûts, étalés sur du court, moyen et long terme, indiquent les dépenses relatives à la mise en œuvre des actions de chacun des 3 plans.

2.1.1. Agence / site « 3725, St-Denis »

	Coûts non récurrents					Coûts récurrents **			Total
	Ressources internes absorbées***	Ressources internes supplém.	Ressources externes	Acquisitions	Sous-total	Ressources internes supplém.	Ressources externes	Sous-total	
Court terme (Année 1)	16 040 $	83 948 $	0 $	20 000 $	103 948 $	58 760 $	0 $	58 760 $	162 708 $
Moyen terme (Année 2)	10 080 $	124 180 $	14 000 $	335 000 $	473 180 $	80 698 $	0 $	80 698 $	553 878 $
Long terme (Année 3)	0 $	46 620 $	0 $	5 000 $	51 620 $	86 693 $	0 $	86 693 $	138 313 $
Total	**26 120 $**	**254 748 $**	**14 000 $**	**360 000 $**	**628 748 $**	**226 151 $**	**0 $**	**226 151 $**	**854 899 $**

2.1.2. Direction de santé publique

	Coûts non récurrents					Coûts récurrents **			Total
	Ressources internes absorbées***	Ressources internes supplém.	Ressources externes	Acquisitions *	Sous-total	Ressources internes supplém.	Ressources externes	Sous-total	
Court terme (Année 1)	73 480 $	135 548 $	75 000 $	568 000 $	778 548 $	52 360 $	0 $	52 360 $	**830 908 $**
Moyen terme (Année 2)	116 200 $	207 900 $	0 $	131 800 $	339 700 $	155 098 $	0 $	155 098 $	**494 798 $**
Long terme (Année 3)	2 800 $	39 620 $	0 $	5 000 $	44 620 $	165 653 $	0 $	165 653 $	**210 273 $**
Total	**192 480 $**	**383 068 $**	**75 000 $**	**704 800 $**	**1 162 868 $**	**373 111 $**	**0 $**	**373 111 $**	**1 535 979 $**

2.1.3. Technocentre régional

	Coûts non récurrents					Coûts récurrents **			Total
	Ressources internes absorbées***	Ressources internes supplém.	Ressources externes	Acquisitions	Sous-total	Ressources internes supplém.	Ressources externes	Sous-total	
Court terme (Année 1)	0 $	115 468 $	0 $	60 000 $	175 468 $	137 040 $	0 $	137 040 $	**312 508 $**
Moyen terme (Année 2)	0 $	138 500 $	0 $	225 000 $	363 500 $	191 412 $	0 $	191 412 $	**554 912 $**
Long terme (Année 3)	0 $	59 220 $	0 $	5 000 $	64 220 $	206 583 $	0 $	206 583 $	**270 803 $**
Total	**0 $**	**313 188 $**	**0 $**	**290 000 $**	**603 188 $**	**535 035 $**	**0 $**	**535 035 $**	**1 138 223 $**

2.1.4. Total des 3 sites (Agence, DSP et TCR)

	Coûts non récurrents					Coûts récurrents **			Total
	Ressources internes absorbées***	Ressources internes supplém.	Ressources externes	Acquisitions	Sous-total	Ressources internes supplém.	Ressources externes	Sous-total	
Court terme (Année 1)	105 560 $	334 964 $	75 000 $	648 000 $	**1 057 964 $**	248 160 $	0 $	**248 160 $**	**1 306 124 $**
Moyen terme (Année 2)	136 360 $	470 580 $	14 000 $	691 800 $	**1 176 380 $**	427 208 $	0 $	**427 208 $**	**1 603 588 $**
Long terme (Année 3)	2 800 $	145 460 $	0 $	15 000 $	**160 460 $**	458 928 $	0 $	**458 928 $**	**619 388 $**
Total	**244 720 $**	**951 004 $**	**89 000 $**	**1 354 800 $**	**2 394 804 $**	**1 134 296 $**	**0 $**	**1 134 296 $**	**3 529 100 $**

***** *Les coûts d'acquisition relatifs au court terme (année 1) incluent un montant de 522 400 $ prévu pour le plan de relève de la DSP.*
****** *Un taux d'indexation de 5 % a été pris en compte dans le calcul des dépenses récurrentes.*
******* *Les coûts des ressources internes absorbées ne sont pas pris en compte dans les coûts totaux. Ils sont uniquement à titre informatif.*

2.2. RÉPARTITION DES COÛTS

Les tableaux en annexe, donnent une répartition détaillée des coûts (récurrents et non récurrents) associés aux ressources humaines. D'une manière générale, la mise en œuvre du plan directeur sollicitera 5 types de ressources :

- **Les ressources relatives à l'exploitation informatique** : Ce sont les ressources affectées à l'exploitation des systèmes informatiques et des réseaux. À la Direction de santé publique, il s'agit de l'équipe de gestion technologique.
- **Les ressources relatives au développement** : Ce sont les ressources impliquées dans la conception, le développement (informatique) et le support des systèmes d'information (SI).
- **Les ressources relatives à la sécurité** : Ce sont les ressources affectées au volet opérationnel de la sécurité des actifs informationnels.
- **Les ressources relatives à la coordination** : Ce sont les ressources responsables de la mise en œuvre et la gestion du plan directeur de la sécurité.
- **Les ressources externes** : Ce sont des ressources externes embauchées par l'Agence soit par manque d'expertise ou de capacité.

2.2.1. Agence / site « 3725, ST-Denis »

(Consulter l'annexe 2.A à la page 12)

2.2.2. Direction de santé publique

(Consulter l'annexe 2.B à la page 13)

2.2.3. Technocentre régional

(Consulter l'annexe 2.C à la page 14)

3. PLANS DIRECTEURS

Les plans directeurs sont les actions à mettre en œuvre sur du court, moyen et long terme, ainsi que les coûts associés à chacune des actions. Chacun des sites de l'Agence a son propre plan directeur.

3.1. PLAN DIRECTEUR DE L'AGENCE

(Consulter l'annexe 3.A à la page15)

3.2. PLAN DIRECTEUR DE LA DIRECTION DE SANTÉ PUBLIQUE

(Consulter l'annexe 3.B à la page 30)

3.3. PLAN DIRECTEUR DU TECHNOCENTRE RÉGIONAL

(Consulter l'annexe 3.C à la page 56)

4. CONCLUSION ET RECOMMANDATIONS

L'élaboration d'un plan directeur de sécurité de l'information demeure tout un défi et demande des efforts soutenus de plusieurs personnes. La gestion et la mise en œuvre du plan directeur doivent être une volonté organisationnelle appuyée par la haute direction. Ce n'est pas uniquement un dossier technologique qui doit être réalisé par les différents services informatiques mais plutôt un dossier de gestion qui doit être appuyé par la haute direction et les différents gestionnaires.

Le document apporte quelques recommandations qui devront être prises en compte par la haute direction :

R1) La mise en œuvre des plans directeurs **DEVRAIT** commencer le plus tôt possible.

R2) Après approbation des plans directeurs par le conseil d'administration, le comité de sécurité des actifs informationnels (CSAI) **DEVRAIT** former un comité dont le mandat serait de prioriser et de planifier (globalement) les projets engendrés par les plans directeurs.

R3) Les ressources responsables de la mise en œuvre du plan (1 analyste en sécurité par site) **DEVRAIENT** être embauchées le plus tôt possible (idéalement pour le mois de septembre 2009), afin d'entamer la planification de la mise en œuvre des plans pour les différents sites.

R4) Les plans de relève informatique pour le TCR et la DSP **DEVRAIENT** être entamés le plus tôt possible. A noter que le plan de relève pour le TCR ne fait pas partie du plan directeur mais plutôt de la planification stratégique de l'Agence.

R5) Étant donné la criticité et la portée (régionale) des actifs informationnels du TCR et de la DSP, les plans directeurs de ces deux sites **DEVRAIENT** être hautement prioritaires.

R6) Pour une gestion uniforme de la mise en œuvre du cadre global de la gestion des actifs informationnels (CGGAI) – volet sécurité au sein de l'Agence, les coordonnateurs responsables (analystes en sécurité) de la mise en œuvre des plans directeurs dans les différents sites **DEVRAIENT** se rapporter à l'officier responsable de la sécurité des actifs informationnels (de l'Agence).

5. ANNEXES

- **Liste des annexes :**

  - **Annexe 2.A** : Répartition des coûts du plan directeur au site « St-Denis »
  - **Annexe 2.B** : Répartition des coûts du plan directeur à la Direction de santé publique
  - **Annexe 2.C** : Répartition des coûts du plan directeur au Technocentre régional
  - **Annexe 3.A** : Plan directeur de la sécurité de l'information pour le site « St-Denis »
  - **Annexe 3.B** : Plan directeur de la sécurité de l'information pour la Direction de santé publique
  - **Annexe 3.C** : Plan directeur de la sécurité de l'information pour le Technocentre

5.1. ANNEXE 2.A : RÉPARTITION DES COÛTS DU PLAN DIRECTEUR AU SITE « ST-DENIS »

	Coûts * des ressources humaines ($)														Coûts des acquisitions	TOTAL
	Coûts non-récurrents ($)							Coûts récurrents ($) **						Total (ress. hum.)		
	Exploitation (Systèmes)	Exploitation (Réseaux)	Développement	Sécurité	Coordination de la MEO du plan directeur	Ressources externes	Sous-Total	Exploitation (Systèmes)	Exploitation (Réseaux)	Développement	Sécurité	Ressources externes	Sous-total			
Court terme (Année 1)	17 000 $	2 240 $	1 400 $	9 800 $	53 508 $	0 $	**83 948 $**	31 160 $	15 840 $	2 520 $	9 240 $	0 $	**58 760 $**	**142 708 $**	20 000 $	**162 708 $**
Moyen terme (Année 2)	12 040 $	5 040 $	46 200 $	22 680 $	38 220 $	14 000 $	**138 180 $**	36 078 $	17 752 $	7 406 $	19 462 $	0 $	**80 698 $**	**218 878 $**	335 000 $	**553 878 $**
Long terme (Année 3)	0 $	0 $	8 400 $	0 $	38 220 $	0 $	**46 620 $**	37 882 $	18 640 $	9 736 $	20 435 $	0 $	**86 693 $**	**133 313 $**	5 000 $	**138 313 $**
Total	**29 040 $**	**7 280 $**	**56 000 $**	**32 480 $**	**129 948 $**	**14 000 $**	**268 748 $**	**105 120 $**	**52 232 $**	**19 662 $**	**49 137 $**	**0 $**	**226 151 $**	**494 899 $**	**360 000 $**	**854 899 $**

*** Le taux horaire est de 40 $ et est celui d'un professionnel et inclut les avantages sociaux**

**** Un taux d'indexation de 5 % est pris en compte dans le calcul des coûts récurrents**

5.2. ANNEXE 2.B : RÉPARTITION DES COÛTS DU PLAN DIRECTEUR À LA DIRECTION DE SANTÉ PUBLIQUE

	Coûts * des ressources humaines ($)												Coûts des acquisitions	TOTAL
	Coûts non-récurrents ($)						Coûts récurrents ($) **					Total (ressources)		
	Équipe de gestion technologique	Développement	Sécurité	Coordination de la MEO du plan directeur	Ressources externes	Sous-Total	Équipe de gestion technologique	Développement	Sécurité	Ressources externes	Sous-total			
Court terme (Année 1)	21 560 $	2 800 $	57 680 $	53 508 $	75 000 $	210 548 $	21 280 $	2 800 $	28 280 $	0 $	**52 360 $**	**262 908 $**	568 000 $	**830 908 $**
Moyen terme (Année 2)	96 600 $	55 440 $	17 640 $	38 220 $	0 $	207 900 $	93 744 $	19 460 $	41 894 $	0 $	**155 098 $**	**362 998 $**	131 800 $	**494 798 $**
Long terme (Année 3)	0 $	0 $	1 400 $	38 220 $	0 $	39 620 $	98 431 $	21 833 $	45 389 $	0 $	**165 653 $**	**205 273 $**	5 000 $	**210 273 $**
Total	**118 160 $**	**58 240 $**	**76 720 $**	**129 948 $**	**75 000 $**	**458 068 $**	**213 455 $**	**44 093 $**	**115 563 $**	**0 $**	**373 111 $**	**831 179 $**	**704 800 $**	**1 535 979 $**

*** Le taux horaire est de 40 $ et est celui d'un professionnel et inclut les avantages sociaux**

**** Un taux d'indexation de 5 % est pris en compte dans le calcul des coûts récurrents**

5.3. ANNEXE 2.C : RÉPARTITION DES COÛTS DU PLAN DIRECTEUR AU TECHNOCENTRE RÉGIONAL

	Coûts * des ressources humaines ($)														Coûts des acquisitions	TOTAL
	Coûts non-récurrents ($)							Coûts récurrents ($) **						Total (ress. hum.)		
	Exploitation (Systèmes)	Exploitation (Réseaux)	Développement	Sécurité	Coordination de la MEO du plan directeur	Ressources externes	Sous-Total	Exploitation (Systèmes)	Exploitation (Réseaux)	Développement	Sécurité	Ressources externes	Sous-total			
Court terme (Année 1)	32 040 $	17 360 $	12 000 $	560 $	53 508 $	0 $	115 468 $	97 360 $	21 200 $	8 120 $	10 360 $	0 $	**137 040 $**	**252 508 $**	60 000 $	**312 508 $**
Moyen terme (Année 2)	46 800 $	2 800 $	33 600 $	17 080 $	38 220 $	0 $	138 500 $	118 148 $	32 060 $	19 126 $	22 078 $	0 $	**191 412 $**	**329 912 $**	225 000 $	**554 912 $**
Long terme (Année 3)	2 800 $	0 $	18 200 $	0 $	38 220 $	0 $	59 220 $	125 455 $	33 663 $	24 282 $	23 182 $	0 $	**206 583 $**	**265 803 $**	5 000 $	**270 803 $**
Total	**81 640 $**	**20 160 $**	**63 800 $**	**17 640 $**	**129 948 $**	**0 $**	**313 188 $**	**340 963 $**	**86 923 $**	**51 528 $**	**55 620 $**	**0 $**	**535 035 $**	**848 223 $**	**290 000 $**	**1 138 223 $**

*** Le taux horaire est de 40 $ et est celui d'un professionnel et inclut les avantages sociaux**

**** Un taux d'indexation de 5 % est pris en compte dans le calcul des coûts récurrents**

5.4. ANNEXE 3.A : PLAN DIRECTEUR DE LA SÉCURITÉ DE L'INFORMATION POUR LE SITE « ST-DENIS »

					Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
1	Budget et ressources alloués à la sécurité	L'organisme dispose de ressources humaines et financières pour gérer la sécurité et la PRP.	C	CT	0	53508	0	5000	58508	0	0	0	58508	Salaire annuel pour une personne qui gère la mise en œuvre du plan directeur de sécurité. Une prime de 5 % du salaire est rajoutée. La personne sera sollicitée pour cette action à 70 %. Le 30 % sera attribué aux autres actions de sécurité. 5000 $ pour la formation et le perfectionnement.
2	Bilan annuel de la sécurité	Un rapport annuel de l'état du dossier de la sécurité de l'information est préparé.	S	CT	0	0	0	0	0	2800	0	2800	2800	70h/année par site
3	Gestion des accès aux locaux informatiques	Les accès sont correctement gérés (attribution, retrait et journalisation des accès).	S	CT	0	0	0	10000	10000	560	0	560	10560	Mise en place d'un système de contrôle d'accès automatique (10000 $). Le coût de la mise en place inclut le système d'accès, la machine, son installation et la formation Rédaction/MAJ de la procédure/directive (14h)
4	Gestion des accès aux locaux informatiques	Un registre de personnes autorisées à accéder aux locaux informatiques est utilisé consignant l'énumération des tâches autorisées pour chacune d'entre elles, et la durée habituelle de leur intervention.	S	CT	0	0	0	0	0	560	0	560	560	Rédaction/MAJ du document
5	Contrôle de l'exploitation (production informatique)	Des procédures d'exploitation sont présentes pour les opérateurs et sont à jour.	ES	CT	4000	5800	0	0	5800	1400	0	1400	7200	Rédaction/MAJ de directives/guides: 35h (récurrent). Rédaction des procédures: 35h * 5 analystes. Mise en place des procédures (70h non-récurrent)
6	Anti-codes malicieux pour les postes de travail	Les utilisateurs connaissent les procédures à suivre en cas d'incidents.	S	CT	0	0	0	0	0	560	0	560	560	Sensibilisation: 14h/année (récurrent)
7	Sauvegarde de sécurité des données et des systèmes présents	Dans le cas extraordinaire où des informations sensibles sont entreposées sur les postes de travail,	ES	CT	0	1400	0	0	1400	280	0	280	1680	Rédaction (35h). MAJ de la directive/procédure (7h)

# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
					Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
	sur les postes de travail	des procédures de sauvegarde ont été rédigées pour les postes de travail des utilisateurs et prévoit la sauvegarde périodique des données.												
8	Sauvegarde de sécurité des données et des systèmes présents sur les postes de travail	Ces procédures ont été distribuées aux utilisateurs.	ES	CT	0	0	0	0	0	0	0	0	0	
9	Protection des portatifs	Par défaut, les données sensibles stockées dans des portatifs sont chiffrées.	ES	CT	0	0	0	0	0	0	0	0	0	Inclus dans la solution de chiffrement.
10	Protection des portatifs	Les utilisateurs sont sensibilisés à ne pas laisser sans surveillance leur portatif et à assurer leur protection.	S	CT	0	0	0	0	0	560	0	560	560	Sensibilisation: 14h/année (récurrent)
11	Intégration de la sécurité dans le développement et l'acquisition des S.I	La certification préalable par le MSSS est nécessaire pour les applications partageables inter sites par l'intermédiaire d'un réseau de télécommunication.	S	CT	0	0	0	0	0	0	0	0	0	Les directives proviennent du MSSS
12	Activités de développement et d'acquisition des systèmes d'information)	Lorsque le développement d'application est confié à un fournisseur externe, le contrat de service exige le respect de ces normes et procédures.	S	CT	0	0	0	0	0	0	0	0	0	Mesure en cours de réalisation avec le service informatique.
13	Gestion de la documentation (maintenance et développement informatique)	Une documentation par application est maintenue à jour et comporte les instructions d'exploitation, de sécurité, de reprise et d'intervention sur anomalie.	D	CT	0	0	0	0	0	560	0	560	560	Mesure déjà implantée. 14h de récurrence par année
14	Contrôle des changements aux applications	Des mécanismes assurent le contrôle des changements sécuritaire des applications.	D	CT	1400	1400	0	0	1400	560	0	560	1960	Mise en place des mécanismes (14h), Rédaction / révision des mécanismes (35h récurrent)

					Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
15	Contrôle des changements aux applications	Ces mécanismes requièrent la mise a jour de la documentation après modification.	D	CT	0	0	0	0	0	0	0	0	0	Inclut dans la mesure 01.C.02.04.01
16	Programme de sensibilisation et de formation	Un programme a été élaboré pour sensibiliser le personnel à la sécurité des actifs informationnels de l'organisme et de la PRP.	S	CT	0	0	0	5000	5000	1400	0	1400	6400	Ce contrôle est couvert dans les 15 mesures obligatoires. Les coûts d'acquisition incluent des outils de sensibilisation tels que les "posters" ou d'autres types d'affiches. La MAJ de 35h est récurrente
17	Programme de sensibilisation et de formation	Ce programme, ou tout autre programme de sensibilisation, inclut les dimensions liées à la protection des renseignements personnels.	S	CT	0	2800	0	0	2800	0	0	0	2800	Inclure la dimension PRP au programme
18	Programme d'accueil des employés	Le programme d'accueil prévoit la présence d'éléments concernant la sécurité informatique et la PRP. (Signature d'un code d'éthique, l'explication de l'importance de la protection des renseignements pour l'organisme, remise de la politique de sécurité, et	S	CT	0	0	0	0	0	0	0	0	0	Inclus dans le programme de sensibilisation
19	Programme de mutation ou de départ des employés	Des mécanismes permettent d'éliminer les accès physiques aux locaux informatiques des personnes qui quittent l'organisme ou changent de fonction, incluant les responsabilités lors de fins de contrat.	S	CT	0	1400	0	0	1400	560	0	560	1960	Implantation des mécanismes (35h). Rédaction/MAJ des mécanismes (14h en récurrent)
20	Programme de mutation ou de départ des employés	Des mécanismes permettent de s'assurer que les employés et contractuels qui quittent l'organisme restituent les biens et les actifs	S	CT	0	0	0	0	0	560	0	560	560	Inclus dans la mesure 02.A.02.02.01

# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
					Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
		informationnels en leur possession.												
21	Architecture redondante et sécuritaire (réseau)	Une revue formelle est effectuée périodiquement afin d'identifier les vulnérabilités du réseau de l'organisme et des équipements de support (alimentation électrique, etc.).	ER	CT	0	0	0	0	0	1960	0	1960	1960	Rédaction/MAJ de procédures/directives (35h). Revue formelle des vulnérabilités 14h en récurrent).
22	Sécurité des réseaux internes	Une analyse est réalisée périodiquement sur la sensibilité et une évaluation formelle est faite périodiquement sur la perméabilité des différents segments du réseau interne et faire évoluer les dispositifs de sécurité en conséquence.	ER	CT	0	0	0	0	0	2800	0	2800	2800	Rédaction/MAJ de procédure/directive : 35h. Analyse des segments: 35h/année (récurrent)
23	Contrôle des accès aux réseaux	Des mécanismes rigoureux et documentés encadrent la création et la modification des codes d'accès utilisés pour gérer ou utiliser les équipements réseau.	ER	CT	1400	1400	0	0	1400	1400	0	1400	2800	Implantation des mécanismes (70h). Rédaction/MAJ des mécanismes (14h en récurrent)
24	Contrôle des accès aux réseaux	Toutes les créations ou modifications de codes d'accès ainsi que les changements aux dispositifs de sécurité réseau sont journalisées et analysées.	ER	CT	0	0	0	0	0	560	0	560	560	Inclus dans la mesure #25
25	Contrôle des accès aux réseaux	Des dispositifs permettent le déclenchement d'alarme associée à certains évènements (tentatives d'accès infructueuses).	ER	CT	0	0	0	0	0	0	0	0	0	Inclus dans l'acquisition de l'outil de surveillance
26	Revue des journaux de sécurité et enquête pour les réseaux	Un examen régulier est effectué par une personne désignée sur les journaux des composantes du réseau qui a été préalablement	ER	CT	1400	0	0	0	0	4440	0	4440	4440	Rédaction de directive/procédure (35h). MAJ de la procédure (7h en récurrent). Examen régulier des journaux: 2h/sem. ou 104/année

# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
					Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
		configuré pour enregistrer les événements de sécurité.												
27	Protection de l'application de messagerie	Les utilisateurs sont sensibilisés à l'impact sur la performance des systèmes de messagerie de la transmission de chaînes de lettres Électroniques et autres types de courrier non sollicités.	ES	CT	0	0	0	0	0	280	0	280	280	Sensibilisation : 7h/année
28	Gestion des privilèges du personnel de support réseau	Les privilèges d'accès du personnel informatique aux ressources réseau sont limités et contrôlés.	ER	CT	0	0	0	0	0	560	0	560	560	Inclus dans la mesure #25
29	Administration des équipements réseau	Un code d'accès unique a été attribué à chacun des administrateurs.	ER	CT	0	0	0	0	0	560	0	560	560	Inclus dans la mesure #25
30	Administration des équipements réseau	Une revue formelle est effectuée périodiquement sur les paramètres de sécurité des équipements réseau et de télécommunication lors des mises en production.	ER	CT	0	0	0	0	0	2800	0	2800	2800	Rédaction/MAJ de la procédure/directive : 35h. Revue formelle des paramètres: 35h/année
31	Administration des équipements réseau	Un journal permet de consigner toutes les interventions de maintenance matérielle et logicielle, la nature des modifications, le nom et la signature de l'intervenant.	ER	CT	560	840	0	0	840	280	0	280	1120	Rédaction (35h) MAJ : 7h (récurrent)
32	Administration des équipements réseau	Le contrôle des accès aux ports de diagnostic et de configuration est adéquat.	ER	CT	560	0	0	0	0	0	0	0	0	
33	Sauvegarde des configurations réseau	Les copies de sauvegarde (exécutables et paramètres de configuration) sont testés périodiquement.	ER	CT	560	0	0	0	0	480	0	480	480	Rédaction de la procédure/directive (35h). MAJ (7h en récurrent). Tests périodiques des copies de sauvegarde: 1h/mois
34	Identification des ressources au serveur (contrôle des accès au	Chaque personne qui accède le serveur possède un code d'accès unique.	ES	CT	280	0	0	0	0	280	0	280	280	Assignation de codes d'accès uniques. Audit annuel (7h en récurrent)

# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
					Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
	serveur)													
35	Identification des ressources au serveur (contrôle des accès au serveur)	Des dates d'expiration sont prévues pour le personnel temporaire.	ES	CT	0	0	0	0	0	0	0	0	0	NA
36	Identification des ressources au serveur (contrôle des accès au serveur)	Les événements importants sont journalisés et vérifiés (tentatives multiples infructueuses, modification des règles de gestion des codes d'accès).	ES	CT	560	840	0		840	4160	0	4160	5000	Mise en place de la journalisation (70h). Vérification des journaux (2h/semaine en récurrent).
37	Identification des ressources au serveur (contrôle des accès au serveur)	Une revue périodique des codes d'accès définis sur le serveur est réalisée. Les codes d'accès n'ayant pas été utilisés depuis un an doivent être désactivés ou détruits.	ES	CT	0	0	0	0	0	1400	0	1400	1400	Revue formelle des codes d'accès: 35h/année
38	Gestion des profils d'accès pour le serveur	Toute création ou modification des règles d'authentification est journalisée dans un registre maintenu à jour.	ES	CT	0	280	0	0	280	0	0	0	280	Rédaction
39	Gestion des profils d'accès pour le serveur	Les profils d'accès sont révisés périodiquement permettant de suspendre, révoquer, bloquer ou radier les privilèges d'accès	ES	CT	0	0	0	0	0	0	0	0	0	Inclus dans la mesure 03.B.01.01.10
40	Gestion des profils d'accès pour le serveur	Des profils d'accès regroupent des rôles ou fonctions précises et régissent les autorisations d'accès aux systèmes. Ces profils ont été créés par les détenteurs. Les accès aux services et aux transactions sont attribués selon les fonctions des personnes.	ES	CT	0	2800	0	0	2800	280	0	280	3080	Mise en place (35h). Rédaction (35h). MAJ (7h en récurrent)
41	Gestion des profils d'accès pour le serveur	Un contrôle rigoureux est effectué sur le processus d'assignation, de	ES	CT	560	840	0	0	840	1400	0	1400	2240	Mise en place (35h). Rédaction/MAJ (35h en récurrent)

# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
					Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
		modification et de retrait de droits d'accès.												
42	Journalisation et gestion des incidents au niveau du serveur	Des mesures et des analyses de performance sont effectuées régulièrement sur le serveur afin de faciliter la détection d'anomalies.	ES	CT	0	0	0	0	0	2080	0	2080	2080	Mise en place de la mesure (COMPLÉTÉE) Analyse périodique : 1h/semaine (en récurrent)
43	Revue des journaux de sécurité et enquête au niveau du serveur	Les journaux de sécurité des systèmes supportant chaque processus d'affaires ayant obtenu une cote 3 ou 4 pour les dimensions de disponibilité, d'intégrité ou de confidentialité sont vérifiés périodiquement. Les types d'événements devant être journalisés	ES	CT	0	0	0	0	0	2360	0	2360	2360	Vérification des journaux : 2h/mois. Rédaction/révision (35h en récurrent)
44	Revue des journaux de sécurité et enquête au niveau du serveur	Un examen régulier est effectué sur les journaux des composantes du serveur qui a été préalablement configuré pour enregistrer les événements de sécurité.	ES	CT	560	840	0	0	840	2080	0	2080	2920	Rédaction de directive/procédure : 35h, Vérification, Vérification: 1h/semaine
45	Gestion des serveurs	Une configuration standard et sécuritaire a été définie, documentée et est adéquatement appliquée au serveur : Suppression de comptes génériques - Paramètres de contrôle des codes d'accès - Paramètres de contrôle des mots de passe - Protection des fichier	ES	CT	1400	1400	0	0	1400	560	0	560	1960	Rédaction (70h). MAJ (14h en récurrent).
46	Gestion des serveurs	Tous les services/ports superflus sont désactivés.	ES	CT	0	0	0	0	0	1400	0	1400	1400	Diagnostic (35h en récurrent)
47	Gestion des serveurs	Un audit périodique (entre autres des tests d'intrusion et des analyses de vulnérabilités) est effectué périodiquement.	ES	CT	0	0	0	0	0	1680	0	1680	1680	Préparation de l'audit : 35h. Audit: 7h/année

# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
					Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
48	Gestion de la maintenance des équipements (serveurs)	Un calendrier de maintenance a été élaboré et tient compte de tous les équipements.	ES	CT	2800	2800	0	0	2800	840	0	840	3640	70h en récurrent
49	Gestion de la maintenance des équipements (serveurs)	Des mécanismes permettent de gérer la mise au rebut sécuritaire des équipements, incluant l'effacement des données confidentielles	S	CT	0	0	0	0	0	280	0	280	280	Rédaction (EN COURS). MAJ (7h en récurrent)
50	Gestion de la maintenance des équipements (serveurs)	Un calendrier et un registre sont suivis indiquant les interventions relatives à la maintenance logicielle, la nature des modifications, le nom et la signature de l'intervenant.	ES	CT	0	0	0	0	0	0	0	0	0	Inclus dans la mesure 03.B.02.03.01
51	Gestion des profils d'accès à l'application	Toute création ou modification des règles d'authentification est journalisée dans un registre maintenu à jour.	D	CT	0	0	0	0	0	0	0	0	0	
52	Gestion des profils d'accès à l'application	Les profils d'accès sont révisés périodiquement permettant de suspendre, révoquer, bloquer ou radier les privilèges d'accès.	D	CT	0	0	0	0	0	560	0	560	560	Révision des profils d'accès: 14h/année
53	Gestion des profils d'accès à l'application	Un processus est présent pour la mise a jour du registre des droits d'accès lors du départ d'un membre du personnel ou lors d'un changement de fonction.	D	CT	0	0	0	0	0	280	0	280	280	Inclus dans la directive de gestion des accès.
54	Revue des journaux de sécurité et enquête pour l'application	Un examen régulier est effectué sur les journaux des composantes de l'application qui a été préalablement configuré pour enregistrer les événements de sécurité.	D	CT	0	0	0	0	0	560	0	560	560	14h/année
55	Copies de sécurité de la base de données	Les copies de sécurité sont révisées périodiquement.	ES	CT	0	0	0	0	0	10680	0	10680	10680	Inclus dans la procédure de prise de copie. MAJ de directive (7h). Vérification des copies de sécurité :

					Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
														5h/semaine en récurrent
56	Contrôles de protection des données en lecture	Les options de menus et transactions de l'application permettant d'accéder en modification aux données des processus catégorisés 3 ou 4 sont attribuées à des personnes autorisées selon leurs fonctions.	D	CT	0	0	0	0	0	0	0	0	0	
57	Ententes et relations avec les fournisseurs	Des engagements sont inclus dans les contrats relativement à la sécurité stipulant et respectent les standards en vigueur et les exigences ministérielles, régionales et locales. Ces engagements inclus notamment : Le respect de la confidentialité, ...	S	CT	0	5600	0	0	5600	1400	0	1400	7000	Mise en place (140h). Révision/MAJ (35h en récurrent)
				Sous-total	**16040**	**83948**	**0**	**20000**	**103948**	**58760**	**0**	**58760**	**162708**	
									0					
58	Budget et ressources alloués à la sécurité	L'organisme dispose de ressources humaines et financières pour gérer la sécurité et la PRP.	C	MT	0	38220	0	5000	43220	0	0	0	43220	Salaire annuel pour une personne qui gère la mise en œuvre du plan directeur de sécurité. Une prime de 5 % du salaire est rajoutée. La personne sera sollicitée pour cette action à 50 %. Le 50 % sera attribué aux autres actions de sécurité. 5000 $ pour la formation et le perfectionnement,
59	Documentation de la gestion de la sécurité	Un manuel de gestion opérationnelle de la sécurité contient l'ensemble des normes, des procédures et des formulaires utilisés.	S	MT	0	5600	0	0	5600	1400	0	1400	7000	Rédaction du manuel (140 h). MAJ/révision (35h récurrents)

					Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
60	Mécanismes de protection des documents électroniques qui transigent sur courrier électronique	Des mécanismes permettant le chiffrement des documents Électroniques qui ont été catégorisés 3 ou 4 pour les dimensions de confidentialité ou d'intégrité sont appliqués lorsque ces documents sont acheminés à l'extérieur du RTSS par courrier Électronique.	ER	MT	0	0	0	0	0	0	0	0	0	Inclus dans la solution de chiffrement.
61	Mécanismes de protection des documents électroniques qui transigent sur courrier électronique	Une procédure écrite est communiquée à cette fin aux utilisateurs pour leur permettre de s'y conformer.	S	MT	0	280	0	0	280	0	0	0	280	Inclus dans la mesure 01.B.01.11.01. Révision de la procédure (7h récurrent))
62	Privilèges du personnel informatique	L'accès aux outils et utilitaires d'administration des systèmes d'exploitation est contrôlé par des mécanismes documentés.	ES	MT	0	5600	0	0	5600	1400	0	1400	7000	Documentation (140h). Révision et MAJ (35h en récurrent),
63	Contrôle de l'exploitation (production informatique)	Un calendrier des tâches à effectuer (cédule de production) est préparé en fonction des besoins définis par le détenteur de l'établissement.	ES	MT	0	1400	0	0	1400	280	0	280	1680	Rédaction de la cédule (140h). Révision/MAJ (35h en récurrent)
64	Contrôle de l'exploitation (production informatique)	Les activités effectuées par les opérateurs sont journalisées et révisées périodiquement.	S	MT	0	5600	0	0	5600	5560	0	5560	11160	Mise en place de la journalisation (140h). Rédaction/MAJ (35h en récurrent). Vérification des journaux : 2h/semaine (récurrent)
65	Mise au rebut des équipements et des supports magnétiques	Les contrats avec les fournisseurs prévoient des clauses spécifiques à cette fin. L'établissement s'assure du respect de ces clauses périodiquement.	S	MT	0	0	0	0	0	0	0	0	0	Inclus dans la mesure 04.A.02.01.05

# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
					Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
66	Haute disponibilité et redondance	Des mécanismes assurent la haute disponibilité et la redondance pour les processus dont la cote de disponibilité a été établie à 4.	ES	MT	0	1400	0	200000	201400	280	0	280	201680	Rédaction de cahier de charges et de spécifications (35h). Révision/MAJ (7h en récurrent). Montant d'acquisition des solutions de haute disponibilité (200 000 $ pour 4 serveurs)
67	Performance du serveur	Pour les processus d'affaires catégorisés 3 ou 4 sur la dimension de la disponibilité, des mécanismes permettent de surveiller la performance du serveur et l'utilisation des ressources afin d'en prévoir la saturation.	ES	MT	1400	1400	0	30000	31400	280	0	280	31680	Mise en place d'outil de surveillance (Outil de surveillance ACEMON acquis). Révision des mécanismes (7h en récurrent).
68	Gestion de la documentation (maintenance et développent informatique)	Des mécanismes permettent de gérer la documentation.	D	MT	1400	1400	14000	20000	35400	280	0	280	35680	Révision des mécanismes (7h récurrent). Les coûts externes correspondent à 70h * 200 $/h = 14000 $
69	Maintenance des applications achetées et supportées par les fournisseurs externes	Des mécanismes permettent de gérer les versions sources des applications obtenues des fournisseurs (ou ces dernières sont placées en fiducie)	D	MT	0	2800	0	0	2800	560	0	560	3360	Mise en place (70h), Rédaction (14h récurrents)
70	Contrôle des accès aux réseaux	Des mécanismes contrôlent les accès au réseau pour les connexions TCP/IP au réseau de l'organisme (pare-feu, routeur, etc.). Mesure du CGGAI no.55) Ces mécanismes permettent de protéger le réseau interne de l'Internet et la configuration de ceux-ci…	ER	MT	0	2800	0	20000	22800	560	0	560	23360	Paramétrage/rédaction (70h). Révision des mécanismes (14h en récurrent)
71	Journalisation et gestion des incidents pour les réseaux	Des mécanismes encadrent la journalisation systématique des tentatives d'accès infructueuses pour tous les équipements réseau.	ER	MT	0	1400	0	0	1400	280	0	280	1680	Inclus dans la solution de journalisation. Révision des mécanismes (7h en récurrent)

					Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
72	Revue des journaux de sécurité et enquête pour les réseaux	Des mécanismes permettent d'effectuer une vérification et des enquêtes en cas de détection d'anomalie. Un processus d'escalade est en place à cette fin.	S	MT	0	5600	0	0	5600	1400	0	1400	7000	Mise en place des mécanismes et interfaçage avec la gestion des incidents (140h).Révision des mécanismes (35h en récurrent)
73	Gestion des privilèges du personnel de support réseau	Des mécanismes contrôlent les modifications ou les ajouts d'outils et utilitaires d'administration réseau.	ER	MT	560	840	0	0	840	280	0	280	1120	Mise en place du mécanisme (70h). Révision du mécanisme (7h en récurrent)
74	Contrôle de la mise en place des systèmes d'exploitation	Une évaluation formelle des spécifications de sécurité du système d'exploitation est effectuée précédant leur mise en place ou présence d'un guide de configuration.	ES	MT	0	0	0	0	0	560	0	560	560	Inclus dans la mesure concernant l'élaboration de la configuration standard pour les serveurs.
75	Contrôle de la mise en place des systèmes d'exploitation	Des mécanismes permettent des tests d'acceptation et des tests de performance si un nouveau système d'exploitation est mis en place.	ES	MT	560	840	0	0	840	280	0	280	1120	Mise en place des mécanismes et rédaction (100h). Révision du mécanisme (20h en récurrent)
76	Contrôle de la mise en place des systèmes d'exploitation	Une vérification systématique de la configuration de sécurité du système d'exploitation est effectuée suite à une nouvelle installation ou à une mise à niveau majeure.	ES	MT	0	0	0	0	0	0	0	0	0	Inclus dans la mesure 03.B.02.02.02
77	Gestion de la maintenance des systèmes (serveurs)	Des mécanismes formels de tests de performance des systèmes sont présents.	ES	MT	0	1400	0	0	1400	280	0	280	1680	Mise en place des mécanismes (35h)
78	Gestion des mécanismes d'authentification à l'application	Les mots de passe doivent être conformes aux exigences minimales du CGGAI/volet sécurité	D	MT	0	33600	0	60 000	93600	0	0	0	93600	Mise en œuvre (840h) / 6 mois. Le coût d'acquisition correspond à l'achat d'un Système d'authentification unique (SSO).

# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
					Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
79	Gestion des mécanismes d'authentification à la base de données	Des procédures assurent la qualité et la solidité du processus d'authentification à la base de données (spécifiant, par exemple, la longueur minimale des mots de passe, la fréquence de leurs changements, la durée de conservation de leur historique etc.).	D	MT	0	0	0	0	0	0	0	0	0	Inclus dans la mesure 03.C.01.02.01
80	Journalisation et gestion des incidents au niveau de la base de données	Des mécanismes encadrent la journalisation systématique des tentatives d'accès infructueuses pour la base de données.	D	MT	2800	5600	0	0	5600	1400	0	1400	7000	Mise en place et rédaction (140h), Révision (35h)
81	Revue des journaux de sécurité et enquête au niveau de la base de données	Les journaux de sécurité des systèmes supportant chaque processus d'affaires ayant obtenu une cote 3 ou 4 pour les dimensions de disponibilité, d'intégrité ou de confidentialité sont vérifiés périodiquement. Les types d'événements devant être journalisés	D	MT	560	1400	0	0	1400	1680	0	1680	3080	Rédaction (35h) /MAJ de procédure/directive (7h). Vérification des journaux : 35h en récurrent
82	Gestion de la base de données supportant les processus	Les changements apportés à la configuration de la base de données sont journalisés et contrôlés.	D	MT	1400	1400	0	0	1400	0	0	0	1400	Interfaçage avec l'outil de journalisation
83	Documentation et schéma de la base de données	La documentation de la base de données a été effectuée et est à jour.	D	MT	0	0	0	0	0	560	0	560	560	Documentation des BD (70h). Révision (14h)
84	Documentation et schéma de la base de données	Les appels d'offre spécifient les critères de documentation de la base de données.	D	MT	1400	0	0	0	0	280	0	280	280	Rédaction de spécifications (35h). Révision (14h),
85	Contrôles de chiffrement des tables de données	Des mécanismes de chiffrement sont définis pour le processus si celui-ci requiert l'entreposage de documents hautement confidentiels (catégorisés à un niveau de 4).	D	MT	0	0	0	0	0	0	0	0	0	Inclus dans la solution de chiffrement.

# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
					Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
86	Contrôles de protection des données en lecture	Les tables et fichiers sont adéquatement protégés en écriture pour les processus catégorisés 3 ou 4 sur la dimension confidentialité. Uniquement les codes d'accès autorisés peuvent accéder les données.	D	MT	0	0	0	0	0	0	0	0	0	Mesure déjà implantée
87	Ententes et relations avec les fournisseurs	Un mécanisme formel a été mis en place afin de régir le choix des tiers et leurs relations.	S	MT	0	5600	0	0	5600	1400	0	1400	7000	Mise en place des mécanismes (140h). Révision du mécanisme (35h en récurrent)
				Sous-total	**10080**	**124180**	**14000**	**335000**	**473180**	**19000**	**0**	**19000**	**492180**	
88	Budget et ressources alloués à la sécurité	L'organisme dispose de ressources humaines et financières pour gérer la sécurité et la PRP.	C	LT	0	38220	0	5000	43220	0	0	0	43220	Salaire annuel pour une personne qui gère la mise en œuvre du plan directeur de sécurité. Une prime de 5 % du salaire est rajoutée. La personne sera sollicitée pour cette action à 50 %. Le 50 % sera attribué aux autres actions de sécurité. 5000 $ pour la formation et le perfectionnement.
89	Gestion des profils d'accès pour le serveur	Des profils d'accès regroupent des rôles ou fonctions précises et régissent les autorisations d'accès aux systèmes. Ces profils ont été créés par les détenteurs. Les accès aux services et aux transactions sont attribués selon les fonctions des personnes.	ES	LT	0	0	0	0	0	0	0	0	0	MESURE DÉJÀ FAITE
90	Revue des journaux de sécurité et enquête pour l'application	Des mécanismes permettent d'effectuer une vérification et des enquêtes en cas de détection d'anomalie.	D	LT	0	0	0	0	0	0	0	0	0	Inclus dans la mesure 03A.01.09.03
91	Interconnexion entre les applications	Des mécanismes de contrôle ont été mis en place afin de protéger l'information lors d'échange d'information	D	LT	0	5600	0	0	5600	1400	0	1400	7000	Mise en place des mécanismes (140h). Révision des mécanismes (35h en récurrent)

					Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
		entre l'application et un système d'information.												
92	Gestion de la base de données supportant les processus	Une configuration standard et sécuritaire a été définie, documentée et est adéquatement appliquée à la base de données. Suppression de comptes génériques - Fermeture de ports non requis et non sécuritaire - Paramètres de contrôle des codes d'accès - Param	D	LT	0	2800	0	0	2800	560	0	560	3360	Élaboration/rédaction du guide (70h), Révision (14h en récurrent)
93	Ententes et relations avec les fournisseurs	Les procédures de choix des tiers incluent une mesure d'analyse de risque et une évaluation des contrôles exercés par les tiers.	S	LT	0	0	0	0	0	0	0	0	0	Inclus dans la mesure 04.A.02.01.02
				Sous-total	**0**	**46620**	**0**	**5000**	**51620**	**1960**	**0**	**1960**	**53580**	

☑ **Le taux horaire de 40 $ est celui d'un professionnel et inclut les avantages sociaux**

*** **Les ressources sollicitées sont : (ES : Exploitation systèmes, ER : Exploitation réseaux, S : Sécurité, D : Développement, C : Coordination)**

+ **CT : court terme, MT : moyen terme, LT : long terme.**

5.5. ANNEXE 3.B : PLAN DIRECTEUR DE LA SÉCURITÉ DE L'INFORMATION POUR LA DIRECTION DE SANTÉ PUBLIQUE

					Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
1	Budget et ressources allouées à la sécurité	L'organisme dispose de ressources humaines et financières pour gérer la sécurité et la PRP.	C	CT	0	53 508	0	5 000	58 508	0	0	0	58 508	Salaire annuel pour une personne qui gère la mise en œuvre du plan directeur de sécurité. Une prime de 5 % du salaire est rajoutée. La personne sera sollicitée pour cette action à 70 %. Le 30 % sera attribué aux autres actions de sécurité. 5000 $ pour la formation et le perfectionnement.
2	Budget et ressources allouées à la sécurité	Ces ressources sont en nombre suffisant.	S	CT	0	0	0	0	0	0	0	0	0	
3	Inventaire, détention et catégorisation des ressources	Un mécanisme a été mis en place pour que les détenteurs révisent annuellement l'inventaire et la catégorisation des actifs et documentent l'utilisation des biens et des informations. (ISO 7.1.3)	S	CT	1 400	1 400	0	0	1 400	1 400	0	1 400	2 800	
4	Analyse de risques	Un mécanisme a été mis en place afin d'évaluer périodiquement les risques et menaces pouvant affecter les actifs informationnels de l'organisme. *(Mesure du Cadre global no.2) Cette évaluation est aussi effectuée lors de modifications majeures de l'environnement technologique de l'organisme, et des suites d'un incident de sécurité. *(Mesure du Cadre global no.2)	S	CT	840	560	0	0	560	1 400	0	1 400	1 960	
5	Analyse de risques	L'analyse de risques est révisée périodiquement.	S	CT	0	0	0	0	0	2 800	0	2 800	2 800	
6	Bilan annuel	Un rapport annuel de l'état du	S	CT	0	0	0	0	0	2 800	0	2 800	2 800	

					Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
	de la sécurité	dossier de la sécurité de l'information est préparé.												
7	Documentation de la gestion de la sécurité	Un manuel de gestion opérationnelle de la sécurité contient l'ensemble des normes, des procédures et des formulaires utilisés.	S	CT	2 800	2 800	0	0	2 800	1 400	0	1 400	4 200	
8	Documentation de la gestion de la sécurité	Les règles concernant la protection des informations et des ressources sont facilement accessibles par les personnes responsables.	S	CT	840	560	0	0	560	280	0	280	840	
9	Normes de gestion de la sécurité	Un registre des actes de gestion de la sécurité permet de consigner tout renseignement obtenu dans le cadre du processus de gestion de la sécurité ainsi que les activités de création de documents, les décisions ou directives en matière de PRP. *(M… Les gestionnaires des différentes unités administratives s'assurent périodiquement du respect, par les employés et le corps professionnel, des normes et procédures en place. (ISO 15.2.1)	S	CT	1 400	1 400	0	0	1 400	840	0	840	2 240	établir et implanter un registre
10	Gestion des crises	Un plan de gestion des crises a été préparé contenant les noms et coordonnées des différents intervenants et les actions urgentes à effectuer selon les situations. Ce plan de crise décrit les situations de crise touchant les systèmes informatiques et traite des aspects spécifiques à ceux-ci. (ISO 14.1.4)	S	CT	1 400	1 400	0	0	1 400	840	0	840	2 240	établir et implanter un plan de gestion de crise
11	Sauvegarde des configurations réseau	Un mécanisme a été mis en place pour la gestion des rustines pour l'ensemble des serveurs/logiciels d'exploitation et anti-codes malicieux. Ce mécanisme prévoit des	EGT	CT	840	560	0	0	560	560	0	560	1 120	établir et implanter le mécanisme

					Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
		activités formelles de veille technologique.												
12	Plans de relève	Pour chacun de ces systèmes, les ressources clé de nature matérielle, logicielle ou humaine ont été identifiées. (ISO 14.1.1)	S	CT	840	560	0	0	560	560	0	560	1 120	
13	Plans de relève	Des plans de relève sont en place pour chaque système critique et sont appuyés par un document écrit. *(Mesure du Cadre global no. 38) (ISO 14.1.3) Ces plans de relève concernent toutes les mesures à suivre pour assurer la continuité des services, incluant les mesures « manuelles », et le retour aux opérations normales. (ISO 14.1.4)	S	CT	11 200	22 400	75 000	425 000	522 400	0	0	0	522 400	implanter le site de relève pour le site 1301 Sherbrooke. Diversifier centraux de Bell pour ligne téléphonique
14	Plans de relève	Les plans sont mis à jour annuellement ou au besoin et sont conservés à l'extérieur du site. *(Mesure du Cadre global no.39) (ISO 14.1.5) Ces plans sont testés régulièrement. *(Mesure du Cadre global no.38) (ISO 14.1.5)	S	CT	0	0	0	0	0	5 600	0	5 600	5 600	
15	Protection physique des documents (papiers/sur support Électronique)	Les documents papiers et sur support électronique sont rangés de manière sécuritaire lors de l'absence des personnes autorisées à les manipuler. (ISO 11.3.3)	S	CT	560	840	0	0	840	560	0	560	1 400	sensibiliser et documenter
16	Contrôle d'emprunt des documents (papiers/sur support Électronique)	Un mécanisme assure le contrôle de la sortie des documents en dehors de l'unité administrative. Le mécanisme permet de garder une trace des documents sortis et les personnes les ayant empruntés.	S	CT	1 400	1 400	0	0	1 400	840	0	840	2 240	établir, documenter et diffuser
17	Contrôle d'emprunt des documents (papiers/sur	Des mécanismes permettent de s'assurer qu'uniquement une partie du dossier est transportée à l'extérieur de l'établissement	S	CT	1 400	1 400	0	0	1 400	840	0	840	2 240	établir, documenter et diffuser

					Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
	support Électronique)	par les utilisateurs ou les personnes autorisées.												
18	Mécanisme de protection des documents Électroniques transitant sur courrier Électronique	Les documents pour lesquels une cote de 3 ou 4 a été attribuée pour une des trois dimensions de DIC sont adéquatement protégées par des mécanismes robustes (chariots barrés, enveloppes cachetées) lorsqu'ils circulent d'une unité administrative à u...	S	CT	1 400	1 400	0	0	1 400	560	0	560	1 960	définir et appliquer (DCIMI)
19	Mécanismes de récupération des documents papiers	Des mécanismes sont prévus afin de récupérer les documents papiers suite à une inondation ou un incendie.	S	CT	1 360	4 200	0	10 000	14 200	840	0	840	15 040	Pour archives et voute.
20	Prévention et détection des inondations des endroits entreposant des documents papiers ou sur supports Électroniques	Les locaux sont munis de dispositifs visant l'évacuation de l'eau en cas de risques d'inondation.	S	CT	560	840	0	10 000	10 840	0	0	0	10 840	Pour archives, voute et salle de serveurs principale.
21	Prévention et détection des inondations des endroits entreposant des documents papiers ou sur supports Électroniques	Des détecteurs d'humidité sont situés à proximité des ressources sensibles.	S	CT	560	840	0	3 000	3 840	0	0	0	3 840	Installer détecteurs: archives, voute, salles des serveurs, satellites
22	Prévention et détection des incendies des endroits entreposant des documents papiers ou sur supports Électroniques	Les locaux contenant des documents sensibles disposent d'un dispositif d'extinction d'incendie, incluant des extincteurs manuels.	S	CT	560	840	0	100 000	100 840	0	0	0	100 840	Pour archives, voute et salle de serveurs principale.
23	Prévention et détection des	Les locaux contenant des documents sensibles sont	S	CT	560	840	0	15 000	15 840	0	0	0	15 840	voûte et archives

					Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
	incendies des endroits entreposant des documents papiers ou sur supports Électroniques	munis de systèmes de chauffage, de ventilation, de contrôle de température et de climatisation adéquats.												
24	Privilèges du personnel informatique	L'accès aux outils et utilitaires d'administration des systèmes d'exploitation est contrôlé par des mécanismes documentés.	S	CT	840	560	0	0	560	0	0	0	560	Établir et documenter
25	Privilèges du personnel informatique	Les conditions d'accès du personnel informatique aux informations sensibles ou confidentielles sont définies dans le cadre de leurs activités quotidiennes d'administration et d'exploitation. *(Mesure du Cadre global no.32)	S	CT	1 400	1 400	0	0	1 400	840	0	840	2 240	Établir, documenter et diffuser
26	Contrôle de l'exploitation	Des procédures d'exploitation sont présentes pour les opérateurs et sont à jour. (ISO 10.1.1)	EGT	CT	1 400	2 800	0	0	2 800	1 400	0	1 400	4 200	Établir, documenter et diffuser
27	Contrôle de l'exploitation	Un calendrier des taches à effectuer (cédule de production) est préparé en fonction des besoins définis par le détenteur de l'établissement. *(Mesure du Cadre global no.31)	EGT	CT	1 400	1 400	0	0	1 400	840	0	840	2 240	Établir, documenter et diffuser
28	Contrôle de l'exploitation	Les activités effectuées par les opérateurs sont journalisées et révisées périodiquement. (ISO 10.10.4)	EGT	CT	1 400	1 400	0	0	1 400	1 400	0	1 400	2 800	Documenter
29	Contrôle de la conformité des configurations des postes de travail	La configuration de base des postes de travail est sécuritaire et documentée. Elle s'inspire des meilleures pratiques.	EGT	CT	840	560	0	0	560	0	0	0	560	documenter
30	Sauvegarde de sécurité des données présentes sur les serveurs	Un plan de sauvegarde et de récupération de l'application, du système d'exploitation et des données a été élaboré pour le processus d'affaires,	EGT	CT	1 400	0	0	0	0	4 200	0	4 200	4 200	Établir, documenter

					Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
		spécifiant la fréquence des copies de sécurité, le lieu d'entreposage de celles-ci, les personnes responsables. Une sauvegarde périodique est effectuée pour les logiciels et les données de l'environnement d'exploitation de ce processus d'affaires.												
31	Sauvegarde de sécurité des données présentes sur les serveurs	Les copies de sauvegarde des programmes sont entreposées ainsi que les fichiers critiques et leur documentation dans un site sécuritaire interne et externe. *(Mesure du Cadre global no.35)	EGT	CT	1 400	1 400	0	0	1 400	840	0	840	2 240	vérifier et documenter
32	Sauvegarde de sécurité des données présentes sur les serveurs	Ces copies de sauvegarde permettent la reconstitution de l'environnement d'exploitation du processus d'affaires.	EGT	CT	1 400	1 400	0	0	1 400	1 400	0	1 400	2 800	vérifier et documenter
33	Sauvegarde de sécurité des données présentes sur les serveurs	L'ensemble de ces procédures et plans de sauvegarde de programmes et de données sont vérifiés régulièrement selon les besoins des utilisateurs. *(Mesure du Cadre global no.36)	EGT	CT	1 400	1 400	0	0	1 400	840	0	840	2 240	Établir et documenter
34	Sauvegarde des systèmes et des données pour les postes de travail	Dans le cas extraordinaire où des informations sensibles sont entreposées sur les postes de travail, des procédures de sauvegarde ont été rédigées pour les postes de travail des utilisateurs et prévoit la sauvegarde périodique des données. *(Mesure du CGGAI)	EGT	CT	1 400	1 400	0	0	1 400	1 400	0	1 400	2 800	Établir, documenter et diffuser
35	Reprise des activités	Des mécanismes de reprise des activités sont prévus pour chaque processus d'affaires ayant obtenu une cote de 3 ou 4 sur la dimension disponibilité suite à l'exercice de catégorisation des actifs informationnels.	S	CT	2 800	2 800	0	0	2 800	1 400	0	1 400	4 200	Établir et documenter

					Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
36	Reprise des activités	Des mécanismes permettent de vérifier la qualité des plans de reprise des activités.	EGT	CT	1 400	1 400	0	0	1 400	1 400	0	1 400	2 800	Établir et documenter
37	Protection des portatifs	Les portatifs sont inventoriés, les utilisateurs possédant ces portatifs sont identifiés et les prêts sont contrôlés. *(Mesure du Cadre global no.15)	EGT	CT	840	560	0	0	560	280	0	280	840	documenter
38	Protection des portatifs	Par défaut, les données sensibles stockées dans des portatifs sont chiffrées.	EGT	CT	1 400	1 400	0	0	1 400	840	0	840	2 240	Établir, documenter et diffuser
39	Protection des portatifs	Des procédures et directives permettent de protéger les équipements hors site, en tenant compte des différents risques associés au travail hors site. (ISO 9.2.5)	EGT	CT	1 400	0	0	0	0	280	0	280	280	Établir, documenter et diffuser
40	Protection des portatifs	Les équipements laissés sans surveillance disposent de mécanismes de protection appropriés, entre autres des câbles de sécurité. *(Mesure du Cadre global no.16) (ISO 11.3.2)	EGT	CT	840	0	0	0	0	280	0	280	280	Établir, documenter et diffuser
41	Gestion de la documentation	Une documentation par application est maintenue à jour et comporte les instructions d'exploitation, de sécurité, de reprise et d'intervention sur anomalie. *(Mesure du Cadre global no.48)	D	CT	2 800	2 800	0	0	2 800	2 800	0	2 800	5 600	Établir, documenter et diffuser
42	Programme de sensibilisation	Ce programme est réévalué périodiquement et au besoin. *(Mesure du Cadre global no.64)	S	CT	0	0	0	0	0	560	0	560	560	Établir, documenter et diffuser
43	Sauvegarde des configurations réseau	Les copies de sauvegarde (exécutables et paramètres de configuration) sont testés périodiquement.	EGT	CT	1 400	0	0	0	0	1 400	0	1 400	1 400	définir et appliquer
44	Identification des ressources au serveur	Pour les applications sensibles (cote d'intégrité ou de confidentialité de 4), une période de connexion maximale a été établie au-delà	EGT	CT	1 400	1 400	0	0	1 400	840	0	840	2 240	établir processus

					Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
		de laquelle les utilisateurs (ou les programmes en lot) doivent s'authentifier à nouveau. *(Mesure du CGGAI...												
45	Identification des ressources au serveur	Les codes d'accès sont désactivés suite à 5 tentatives infructueuses consécutives. *(Mesure du Cadre global no.19)	EGT	CT	840	0	0	0	0	0	0	0	0	documenter
46	Identification des ressources au serveur	Une revue périodique des codes d'accès définis sur le serveur est réalisée. Les codes d'accès n'ayant pas été utilisés depuis un an doivent être désactivés ou détruits. *(Mesure du Cadre global no.23) (ISO 11.2.4)	EGT	CT	1 280	560	0	0	560	560	0	560	1 120	établir processus
47	Identification des ressources au serveur	Une procédure est en place afin de détruire les codes d'accès lorsque la personne s'absente pour une période de plus de six semaines ou si elle quitte définitivement l'organisme. *(Mesure du Cadre global no.20) (ISO 11.2.1)	EGT	CT	560	0	0	0	0	560	0	560	560	établir processus
48	Gestion des mécanismes d'authentification au serveur	Le choix des mots de passe des utilisateurs respecte les meilleures pratiques. (ISO 11.3.1)	EGT	CT	2 800	2 800	0	0	2 800	0	0	0	2 800	établir processus
49	Gestion des mécanismes d'authentification au serveur	En cas d'oubli du mot de passe, l'identité de l'utilisateur est validée avant d'octroyer un nouveau mot de passe.	EGT	CT	840	0	0	0	0	560	0	560	560	établir processus
50	Gestion des mécanismes d'authentification au serveur	La composition du mot de passe est-elle adéquate et obligatoire. *(Mesure du Cadre global no.28) (ISO 11.5.3) 8 caractères minimum - lettres, chiffres ou caractères spéciaux. Le système garde un historique des dix derniers mots de passe. *(Mesure du Cadre global no.28)	EGT	CT	1 400	0	0	0	0	0	0	0	0	implanter
51	Gestion des profils d'accès	Toute création ou modification des règles d'authentification est	EGT	CT	840	0	0	0	0	560	0	560	560	établir processus

# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
					Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
	au serveur	journalisée dans un registre maintenu à jour.*(Mesure du Cadre global no.21)												
52	Gestion des profils d'accès au serveur	Les profils d'accès sont révisés périodiquement permettant de suspendre, révoquer, bloquer ou radier les privilèges d'accès *(Mesure du Cadre global no.20)	EGT	CT	840	560	0	0	560	560	0	560	1 120	établir processus
53	Gestion des profils d'accès au serveur	Un contrôle rigoureux est effectué sur le processus d'assignation, de modification et de retrait de droits d'accès.	EGT	CT	840	560	0	0	560	280	0	280	840	établir processus
54	Gestion des licences	Présence d'un processus formel de gestion des licences. *(Mesure du Cadre global no.45) (ISO 15.1.2)	S	CT	1 400	2 800	0	0	2 800	1 400	0	1 400	4 200	Établir et implanter processus
55	Présence d'un calendrier de conservation	Présence d'un calendrier de conservation pour tous les documents.	S	CT	1 400	4 200	0	0	4 200	1 400	0	1 400	5 600	Avec Agence
56	Présence d'un calendrier de conservation	Ce calendrier tient compte des documents papier et électroniques. Incluant les journaux de journalisation. *(Mesure du Cadre global no.30)	S	CT	0	0	0	0	0	0	0	0	0	suite
57	Présence d'un calendrier de conservation	Une procédure est en place pour s'assurer du respect du calendrier.	S	CT	1 400	1 400	0	0	1 400	840	0	840	2 240	établir procédure
58	Présence d'un calendrier de conservation	Un libellé est apposé sur les documents afin d'y indiquer la cote de catégorisation.	S	CT	560	840	0	0	840	280	0	280	1 120	établir politique
				Sous-total	**73 480**	**135 548**	**75 000**	**568 000**	**778 548**	**52 360**	**0**	**52 360**	**830 908**	
59	Budget et ressources allouées à la sécurité	L'organisme dispose de ressources humaines et financières pour gérer la sécurité et la PRP.	C	MT	0	38 220	0	5 000	43 220	0	0	0	43 220	Salaire annuel pour une personne qui gère la mise en œuvre du plan directeur de sécurité. Une prime de 5 % du salaire est rajoutée. La personne sera sollicitée pour cette action à 50 %. Le

					Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
														50 % sera attribué aux autres actions de sécurité. 5000 $ pour la formation et le perfectionnement.
60	Gestion des accès aux locaux informatiques	Un mécanisme permettant la restitution des moyens d'accès avant départ ou mutation et modification des accès (si code physique) a été défini.	S	MT	840	0	0	0	0	0	0	0	0	Documenter
61	Gestion des accès aux locaux informatiques	Les accès temporaires sont correctement gérés (attribution, retrait et journalisation des accès).	S	MT	840	0	0	0	0	0	0	0	0	Documenter
62	Gestion des accès aux locaux informatiques	La salle des serveurs de production n'est pas utilisée à des fins de développement. Le personnel de développement et de programmation n'a pas accès à la salle informatique sans être accompagné par une personne autorisée.	S	MT	840	0	0	0	0	0	0	0	0	Documenter
63	Gestion des équipements informatiques	Un inventaire est présent et à jour consignant les équipements informatiques incluant leur localisation et assignation principale. *(Mesure du Cadre global no.10)	EGT	MT	1 400	4 200	0	0	4 200	1 400	0	1 400	5 600	Établir et documenter
64	Gestion des équipements informatiques	Des mécanismes sont utilisés afin de protéger les équipements contre le vol ou l'utilisation non autorisée. Des mécanismes régissent l'emplacement des équipements informatiques, spécifiant que ceux-ci doivent être placés de façon à leur éviter toute utilisation et observation non-autorisées.	S	MT	1 400	1 400	0	0	1 400	840	0	840	2 240	documenter
65	Gestion des équipements informatiques	Des mécanismes régissent la sortie d'équipement hors des installations de l'organisme, requérant une autorisation appropriée et l'analyse	S	MT	280	560	0	0	560	0	0	0	560	Établir et documenter

					Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
		préalable et élimination possible des données contenues sur ces équipements. *(Mesure du Cadre global no.17)												
66	Gestion des équipements informatiques	Des mécanismes assurent le contrôle de la mise au rebut des équipements ayant contenu des données de l'établissement. *(Mesure du Cadre global no.13)	S	MT	840	0	0	0	0	0	0	0	0	Établir et documenter
67	Restriction dans la manipulation de documents à l'extérieur de l'établissement	Des mécanismes permettent de s'assurer qu'uniquement une partie du dossier est transportée à l'extérieur de l'établissement par les utilisateurs ou les personnes autorisées, ce qui permet de limiter les impacts d'une perte du dossier.	S	MT	1 400	1 400	0	0	1 400	560	0	560	1 960	Établir, documenter et diffuser
68	Mécanisme de transport des documents (papiers/sur supports Électroniques) vers l'externe	Lors de l'acheminement de documents confidentiels (3 ou 4) vers un endroit externe, des mécanismes sont en place afin de s'assurer que la personne qui reçoit le document est autorisée et que ce dernier est adéquatement manipulé (par exemple, ne pa…	S	MT	0	0	0	0	0	560	0	560	560	suite
69	Maintenance des applications achetées et supportées par les fournisseurs externes	Des mécanismes permettant le chiffrement des documents électroniques qui ont été catégorisés 3 ou 4 pour les dimensions de confidentialité ou d'intégrité sont appliqués lorsque ces documents sont acheminés à l'extérieur du RTSS par courrier électronique…	S	MT	1 400	1 400	0	800	2 200	560	0	560	2 760	acheter, tester et implanter logiciel centralisé de cryptographie
70	Contrôle des accès aux réseaux	Une procédure écrite est communiquée à cette fin aux utilisateurs pour leur permettre de s'y conformer.	S	MT	1 400	0	0	0	0	280	0	280	280	Établir, documenter et diffuser
71	Prévention et détection des inondations	Les locaux qui hébergent des équipements informatiques sont situés à un endroit adéquat afin de prévenir les dégâts	S	MT	840	560	0	25 000	25 560	0	0	0	25 560	calorifères à eau chaude au-dessus de la salle des serveurs et toilettes le local mitoyen de

# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
					Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
		d'eau. Aucun tuyau d'eau n'est présent dans le plafond de la salle.*(Mesure du Cadre global no.4.1) (ISO 9.1.4)												la salle des serveurs
72	Construction et localisation de la salle informatique	La salle informatique n'est pas située au sous-sol, prés du toit ou près d'une source de risque physique ou d'un accès non autorisé. (ISO 9.2.1)	S	MT	0	0	0	0	0	0	0	0	0	non, mais palié par installation d'une salle de relève
73	Construction et localisation de la salle informatique	La salle dispose d'équipements adéquats de contrôle de chauffage et de vérification de la température.	S	MT	560	840	0	16 000	16 840	0	0	0	16 840	climatisation dans 2 salles satellites
74	Impression sécuritaire et distribution	Des contrôles limitent l'accès aux fonctions d'impression et aux outils de saisie d'image afin d'empêcher l'impression d'informations contenant des renseignements personnels. *(Mesure du Cadre global no.51 et 52)	S	MT	1 400	1 400	0	0	1 400	840	0	840	2 240	Établir, documenter et diffuser
75	Impression sécuritaire et distribution	Les imprimantes sont situées dans un endroit sécuritaire. *(Mesure du Cadre global no.5) et le détenteur en a déterminé le nombre et la localisation. *(Mesure du Cadre global no.53)	S	MT	1 400	1 400	0	0	1 400	1 280	0	1 280	2 680	vérifier et documenter
76	Impression sécuritaire et distribution	Un mécanisme permet la distribution sécuritaire des rapports confidentiels.	S	MT	1 400	1 400	0	0	1 400	840	0	840	2 240	Établir, documenter et diffuser
77	Gestion des supports Électroniques	Des mécanismes permettent d'encadrer l'archivage et l'utilisation des données selon le type de support et le niveau de catégorisation.	S	MT	560	840	0	0	840	560	0	560	1 400	Établir, documenter et diffuser
78	Gestion des supports Électroniques	Des mécanismes permettent de gérer la manipulation des supports électroniques. (ISO 10.7.1 et 10.7.3)	S	MT	560	840	0	0	840	560	0	560	1 400	Établir, documenter et diffuser
79	Gestion des supports Électroniques	Des mécanismes régissent la circulation des supports électroniques et spécifient des mesures de sécurité adéquates. (ISO 10.8.3)	S	MT	0	0	0	0	0	0	0	0	0	suite

					Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
80	Performance du serveur	Pour les processus d'affaires catégorisés 3 ou 4 sur la dimension de la disponibilité, des mécanismes permettent de surveiller la performance du serveur et l'utilisation des ressources afin d'en prévoir la saturation. (ISO 10.3.1)	S	MT	2 800	2 800	0	5 000	7 800	1 400	0	1 400	9 200	installer outil de monitorage et documenter
81	Gestion du personnel stratégique	La documentation du système et des procédures d'opération du système est à jour.	S	MT	1 400	1 400	0	0	1 400	1 400	0	1 400	2 800	Établir et documenter
82	Intégration de la sécurité dans le développement et l'acquisition des systèmes d'information	Une méthodologie de développement d'applications est utilisée intégrant des considérations de sécurité et de PRP et existence de normes et procédures à cet effet. *(Mesure du Cadre global no.44) (ISO 12.1.1)	D	MT	1 400	4 200	0	0	4 200	0	0	0	4 200	Établir, documenter et diffuser
83	Intégration de la sécurité dans le développement et l'acquisition des systèmes d'information	Les besoins en sécurité et en PRP sont formellement identifiés par le détenteur désigné. Une analyse à cette fin doit être effectuée et inclut la catégorisation du nouveau système. (ISO 12.1.1)	D	MT	560	840	0	0	840	280	0	280	1 120	Établir, documenter et diffuser
84	Activités de développement et d'acquisition des systèmes d'information	Lors d'une mise en production, une revue formelle de la documentation des applications est effectuée.	D	MT	0	0	0	0	0	0	0	0	0	Établir, documenter et diffuser
85	Gestion de la documentation	Des mécanismes permettent de gérer la documentation.	D	MT	1 400	1 400	0	0	1 400	840	0	840	2 240	Établir, documenter et diffuser
86	Contrôle des changements aux applications	Ces mécanismes requièrent, des tests par les utilisateurs et une approbation formelle de mise en place par le détenteur. (ISO 12.5.2)	D	MT	0	0	0	0	0	1 400	0	1 400	1 400	
87	Modifications en cas d'urgence	Les modifications en cas d'urgence sont documentées, journalisées et enquêtées.	D	MT	560	840	0	0	840	840	0	840	1 680	Établir, documenter et diffuser
88	Programme de	Des mécanismes visent à	S	MT	560	840	0	0	840	0	0	0	840	Établir, documenter

# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
					Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
	mutation ou de départ des employés	modifier les accès des utilisateurs qui changent de types d'emploi afin de s'assurer qu'ils ne conservent pas leurs privilèges d'accès liés à leurs taches antérieures. (ISO 8.3.3)												et diffuser
89	Architecture redondante et sécuritaire	Une revue formelle est effectuée périodiquement afin d'identifier les vulnérabilités du réseau de l'organisme et des équipements de support (alimentation électrique, etc.).	EGT	MT	560	840	0	0	840	1 400	0	1 400	2 240	documenter
90	Architecture redondante et sécuritaire	Une architecture redondante est présente et vise à palier aux défaillances potentielles du réseau selon les besoins des détenteurs. *(Mesure du Cadre global no.58)	EGT	MT	560	840	0	0	840	0	0	0	840	documenter
91	Architecture redondante et sécuritaire	Des mesures on-line permettent l'équilibrage de la charge réseau.	EGT	MT	560	2 240	0	10 000	12 240	1 400	0	1 400	13 640	documentation et achat de solution
92	Architecture redondante et sécuritaire	Des procédures de reprise permettent de rétablir les activités réseau dans les délais déterminés. *(Mesure du Cadre global no.58)	EGT	MT	1 400	4 200	0	0	4 200	1 400	0	1 400	5 600	rédaction
93	Sécurité des réseaux internes	Un mécanisme formel permet d'identifier les équipements réseau autorisés pour les connexions. *(Mesure du Cadre global no.55) (ISO 11.4.3)	EGT	MT	1 400	1 400	0	0	1 400	1 400	0	1 400	2 800	rédaction, implantation
94	Sécurité des réseaux internes	Une analyse est réalisée périodiquement sur la sensibilité et une évaluation formelle est faite périodiquement sur la perméabilité des différents segments du réseau interne *(Mesure du Cadre global no.57) (ISO 10.6.1)…	EGT	MT	560	840	0	0	840	1 400	0	1 400	2 240	rédaction
95	Sécurité des réseaux internes	Des mécanismes permettent de gérer formellement la configuration des équipements réseau. (ISO 10.6.2)	EGT	MT	1 400	1 400	0	0	1 400	1 400	0	1 400	2 800	rédiger et implanter

					Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
96	Contrôle des accès aux réseaux	Des mécanismes rigoureux et documentés encadrent la création et la modification des codes d'accès utilisés pour gérer ou utiliser les équipements réseau. *(Mesures du Cadre global no.57 et no.18) (ISO 11.4.6 et 11.1.1)	EGT	MT	1 400	1 400	0	0	1 400	1 400	0	1 400	2 800	rédiger , implanter
97	Contrôle des accès aux réseaux	Toutes les créations ou modifications de codes d'accès ainsi que les changements aux dispositifs de sécurité réseau sont journalisées et analysées.	EGT	MT	1 400	4 200	0	0	4 200	1 400	0	1 400	5 600	rédiger, implanter et faire suivi
98	Contrôle des accès aux réseaux	Des mécanismes d'audit enregistrent certaines actions d'intérêt (tentatives multiples infructueuses, modification des règles de gestion des codes d'accès).	EGT	MT	1 400	0	0	0	0	1 400	0	1 400	1 400	rédiger, implanter et faire suivi
99	Contrôle des accès aux réseaux	Des dispositifs permettent le déclenchement d'alarme associée à certains événements (tentatives d'accès infructueuses). *(Mesure du Cadre global no.41)	EGT	MT	1 400	2 800	0	5 000	7 800	1 400	0	1 400	9 200	implanter console
100	Contrôle des accès aux réseaux	Des mécanismes contrôlent les accès au réseau pour les connexions TCP/IP au réseau de l'organisme (pare-feu, routeur, etc.). *(Mesure du Cadre global no.55) Ces mécanismes permettent de protéger le réseau interne de l'Internet et la configuration…	EGT	MT	1 400	1 400	0	0	1 400	1 400	0	1 400	2 800	
101	Contrôle des accès aux réseaux	Ce contrôle respecte la logique « tout ce qui n'est pas explicitement permis est interdit ».	EGT	MT	1 400	4 200	0	0	4 200	2 800	0	2 800	7 000	établir et implanter
102	Contrôle des accès aux réseaux	Un nombre limité d'individus sont autorisés à modifier les paramètres de configuration des mécanismes ci-dessus, et contrôle d'accès strict à ces fonctions. Toute modification est journalisée et auditée.	EGT	MT	1 400	0	0	0	0	840	0	840	840	documenter et alimenter

					Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
103	Configuration du système de détection des intrusions	Le personnel devant se servir du système de détection des intrusions est adéquatement formé.	EGT	MT	2 800	0	0	5 000	5 000	0	0	0	5 000	Formation
104	Chiffrement et protection de la confidentialité des informations	Un système de chiffrement est utilisé pour la transmission de données sur le réseau liées à des processus d'affaires qui ont reçu une cote 3 ou 4 pour la dimension confidentialité. L'information doit être mise en mémoire sous forme chiffrée avant …La longueur des clés de chiffrement est adéquate. Des mécanismes adéquats permettent d'assurer la gestion des clés de chiffrement. (ISO 12.3.2)	EGT	MT	1 400	4 200	0	50 000	54 200	1 400	0	1 400	55 600	implantation de solution de chiffrement
105	Journalisation et gestion des incidents pour le réseau	Des mécanismes encadrent la journalisation systématique des tentatives d'accès infructueuses pour tous les équipements réseau. *(Mesure du Cadre global no.41)Les journaux sont protégés afin d'assurer leur intégrité et leur conservation à long terme. (ISO 10.10.3)	EGT	MT	1 400	4 200	0	0	4 200	1 400	0	1 400	5 600	acquisition d'un outil de journalisation
106	Journalisation et gestion des incidents pour le réseau	Des mesures et des analyses de performance sont effectuées régulièrement sur les réseaux afin de faciliter la détection d'anomalies.	EGT	MT	1 400	4 200	0	10 000	14 200	2 800	0	2 800	17 000	implantation outil de monitorage
107	Journalisation et gestion des incidents pour le réseau	Un système enregistre pour chaque incident les informations suivantes : date, heure, nature de l'incident, durée d'indisponibilité, le statut (en cours, en étude, résolu), les mesures correctives apportées, ainsi que le nom de l'intervenant.	EGT	MT	2 800	8 400	0	0	8 400	2 800	0	2 800	11 200	implantation d'un processus de gestion d'incidents
108	Revue des journaux de sécurité et enquête pour	Un examen regulier est effectué par une personne désignée sur les journaux des composantes du réseau qui a	EGT	MT	1 400	0	0	0	0	1 400	0	1 400	1 400	rédaction

					Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
	le réseau	été préalablement configuré pour enregistrer les événements de sécurité. *(Mesure du Cadre global no.42) (ISO 10.10.2)												
109	Revue des journaux de sécurité et enquête pour le réseau	Des mécanismes permettent d'effectuer une vérification et des enquêtes en cas de détection d'anomalie. Un processus d'escalade est en place à cette fin. *(Mesure du Cadre global no.43) (ISO 13.2.3)	EGT	MT	0	0	0	0	0	0	0	0	0	inclus dans gestion des incidents
110	Protection du site WEB et des autres services offerts de l'extérieur	Des procédures ont été définies afin de protéger les informations mises à la disposition du public. (ISO 10.9.3)	EGT	MT	560	840	0	0	840	1 400	0	1 400	2 240	rédaction
112	Gestion des privilèges du personnel de support réseau	Les accès aux utilitaires et outils d'administration des équipements réseau sont contrôlés. (1SO 11.5.4) Des mécanismes contrôlent les modifications ou les ajouts d'outils et utilitaires d'administration réseau.	EGT	MT	1 400	1 400	0	0	1 400	1 400	0	1 400	2 800	rédiger mesure
113	Gestion des privilèges du personnel de support réseau	Une entente de service précise les conditions d'accès du personnel informatique aux informations sensibles ou confidentielles, dans le cadre de leurs activités quotidiennes d'administration et d'exploitation. *(Mesure du Cadre global no.32)	EGT	MT	560	840	0	0	840	560	0	560	1 400	rédiger diffuser
114	Administration des équipements réseau	Un code d'accès unique a été attribué à chacun des administrateurs.	EGT	MT	280	0	0	0	0	0	0	0	0	attribution et révision
115	Administration des équipements réseau	Une configuration type a été définie pour les équipements réseau et permet le contrôle du routage réseau selon les normes et les besoins des systèmes d'information. *(Mesure du	EGT	MT	1 400	1 400	0	0	1 400	1 400	0	1 400	2 800	documenter

					Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
		Cadre global no.11) (ISO 11.4.7) Toutes les modifications apportées à la configuration des équipements réseau sont journalisées et analysées.												
116	Administration des équipements réseau	Une revue formelle est effectuée périodiquement sur les paramètres de sécurité des équipements réseau et de télécommunication lors des mises en production.	EGT	MT	560	840	0	0	840	1 400	0	1 400	2 240	rédaction
117	Administration des équipements réseau	Un journal permet de consigner toutes les interventions de maintenance matérielle et logicielle, la nature des modifications, le nom et la signature de l'intervenant.	EGT	MT	560	0	0	0	0	1 400	0	1 400	1 400	rédaction et suivi
118	Administration des équipements réseau	Tous les services superflus sont désactivés et un mécanisme de durcissement des équipements est suivi.	EGT	MT	560	840	0	0	840	1 400	0	1 400	2 240	rédaction et suivi
119	Administration des équipements réseau	Un audit périodique (entre autres des tests d'intrusion et des analyses de vulnérabilités) est effectué périodiquement. (ISO 15.2.2)	EGT	MT	1 400	1 400	0	0	1 400	1 400	0	1 400	2 800	rédaction et suivi
120	Gestion des changements aux équipements réseau	Une revue formelle est effectuée périodiquement sur les paramètres de sécurité des équipements réseau et de télécommunication lors des mises en production.	EGT	MT	1 400	0	0	0	0	2 800	0	2 800	2 800	établir et implanter
121	Gestion des changements aux équipements réseau	Des tests fonctionnels et des tests de performance sont effectués sur les nouveaux équipements, selon des procédures préétablies.	EGT	MT	1 400	1 400	0	0	1 400	1 400	0	1 400	2 800	rédaction et suivi
122	Gestion des changements aux équipements réseau	Un journal permet de consigner toutes les interventions de maintenance matérielle et logicielle, la nature des modifications, le nom et la signature de l'intervenant.	EGT	MT	1 400	1 400	0	0	1 400	1 400	0	1 400	2 800	établir et implanter
123	Gestion des	Des mécanismes régissent la	EGT	MT	560	840	0	0	840	560	0	560	1 400	rédaction et suivi

					Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
	changements aux équipements réseau	mise au rebut des équipements réseau, spécifiant que tout équipement ayant contenu des informations sensibles doit être détruit.												
124	Sauvegarde des configurations réseau	Un plan de sauvegarde des configurations du réseau local est présent, définissant les objets à sauvegarder et la fréquence de sauvegarde.	EGT	MT	560	840	0	0	840	560	0	560	1 400	définir et appliquer
125	Sécurité physique du câblage réseau	Un dossier permet de connaître les chemins réseau et les emplacements de câblage.	EGT	MT	560	2 240	0	0	2 240	560	0	560	2 800	rédiger
126	Identification des ressources au serveur	Des mécanismes formels et documentés encadrent la gestion des codes d'accès, entre autres la présence d'un formulaire de contrôle d'accès signé par les personnes autorisées et qualifiées. (ISO 11.1.1)	EGT	MT	560	840	0	0	840	560	0	560	1 400	rédiger
127	Identification des ressources au serveur	Les événements importants sont journalisés et vérifiés (tentatives multiples infructueuses, modification des règles de gestion des codes d'accès).	EGT	MT	1 400	1 400	0	0	1 400	1 400	0	1 400	2 800	établir processus
128	Gestion des profils d'accès au serveur	Un nombre limité de personnes sont autorisées à changer les règles d'authentification des utilisateurs et il existe un contrôle strict de l'accès aux fonctions permettant la gestion des règles. (ISO 11.2.1)	EGT	MT	560	840	0	0	840	560	0	560	1 400	documenter
129	Gestion des profils d'accès au serveur	L'attribution de droits à ces différents profils fait l'objet d'une approbation de la part des détenteurs des actifs informationnels concernés. Toute dérogation est approuvée par le détenteur. Un processus est présent pour la mise a jour du registre des droits d'accès lors du départ d'un membre du personnel ou lors d'un	EGT	MT	1 400	0	0	0	0	280	0	280	280	établir processus

# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
					Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
		changement de fonction*.												
130	Journalisation et gestion des incidents au niveau du serveur	Des mécanismes encadrent la journalisation systématique des tentatives d'accès infructueuses pour le serveur.	EGT	MT	2 800	8 400	0	0	8 400	2 800	0	2 800	11 200	établir processus
131	Journalisation et gestion des incidents au niveau du serveur	Les journaux sont protégés afin d'assurer leur intégrité et leur conservation à long terme. (ISO 10.10.3)	EGT	MT	560	840	0	0	840	560	0	560	1 400	établir processus, valider avec le calendrier de conservation
132	Journalisation et gestion des incidents au niveau du serveur	Des mesures et des analyses de performance sont effectuées régulièrement sur le serveur afin de faciliter la détection d'anomalies.	EGT	MT	560	840	0	0	840	560	0	560	1 400	établir processus
133	Journalisation et gestion des incidents au niveau du serveur	Un système enregistre pour chaque incident les informations suivantes : date, heure, nature de l'incident, durée d'indisponibilité, le statut (en cours, en étude, résolu), les mesures correctives apportées, ainsi que le nom de l'intervenant.	EGT	MT	2 800	8 400	0	0	8 400	2 800	0	2 800	11 200	établir processus
134	Revue des journaux de sécurité et enquête au niveau du serveur	Les journaux de sécurité des systèmes supportant chaque processus d'affaires ayant obtenu une cote 3 ou 4 pour les dimensions de disponibilité, d'intégrité ou de confidentialité sont vérifiés périodiquement. Les types d'événements devant être jour...	EGT	MT	560	840	0	0	840	840	0	840	1 680	établir processus
135	Revue des journaux de sécurité et enquête au niveau du serveur	Un examen régulier est effectué sur les journaux des composantes du serveur qui a été préalablement configuré pour enregistrer les événements de sécurité. (ISO 10.10.2)	EGT	MT	0	0	0	0	0	0	0	0	0	suite
136	Revue des journaux de sécurité et enquête au niveau du	Cette surveillance est effectuée à l'aide de logiciels spécialisés.	EGT	MT	0	0	0	0	0	0	0	0	0	suite

# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
					Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
	serveur													
137	Revue des journaux de sécurité et enquête au niveau du serveur	Un examen régulier est effectué sur les journaux des composantes du serveur qui a été préalablement configuré pour enregistrer les événements de sécurité. (ISO 10.10.2)	EGT	MT	0	0	0	0	0	2 800	0	2 800	2 800	établir processus
138	Revue des journaux de sécurité et enquête au niveau du serveur	Des mécanismes permettent d'effectuer une vérification et des enquêtes en cas de détection d'anomalie.	EGT	MT	560	840	0	0	840	2 800	0	2 800	3 640	établir processus
139	Gestion des serveurs	Tous les services/ports superflus sont désactivés.	EGT	MT	840	1 960	0	0	1 960	840	0	840	2 800	établir processus
140	Gestion des serveurs	Les activités de l'administrateur de système sont journalisés et vérifiés périodiquement par une personne indépendante. (ISO 10.10.4)	S	MT	840	560	0	0	560	840	0	840	1 400	établir processus
141	Gestion des serveurs	La documentation sur la configuration du serveur est protégée et accessible aux personnes autorisées. (ISO 10.7.4)	EGT	MT	840	0	0	0	0	280	0	280	280	établir processus
142	Contrôle de la mise en place des systèmes d'exploitation	Une évaluation formelle des spécifications de sécurité du système d'exploitation est effectuée précédant leur mise en place ou présence d'un guide de configuration.	S	MT	1 400	0	0	0	0	1 400	0	1 400	1 400	établir processus
143	Contrôle de la mise en place des systèmes d'exploitation	Une procédure d'installation est présente.	EGT	MT	1 400	0	0	0	0	0	0	0	0	établir processus
144	Contrôle de la mise en place des systèmes d'exploitation	Une vérification systématique de la configuration de sécurité du système d'exploitation est effectuée suite à une nouvelle installation ou à une mise à niveau majeure.	EGT	MT	0	0	0	0	0	840	0	840	840	suite
145	Contrôle de la mise en place des systèmes d'exploitation	La mise a jour de la documentation du système d'exploitation est requise avant la mise en place.	EGT	MT	0	0	0	0	0	840	0	840	840	suite

					Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
146	Gestion de la maintenance des équipements	Un calendrier de maintenance a été élaboré et tient compte de tous les équipements. *(Mesure du Cadre global no.12) (ISO 9.2.4)	EGT	MT	1 400	1 400	0	0	1 400	840	0	840	2 240	établir processus
147	Gestion de la maintenance des équipements	Un registre de suivi a été mis en place indiquant les interventions relatives à la maintenance matérielle, la nature des modifications, le nom et la signature de l'intervenant. (ISO 9.2.4)	EGT	MT	0	0	0	0	0	0	0	0	0	suite
148	Gestion de la maintenance des équipements	Des mécanismes de maintenance préventive des équipements sont présents. Un contrat de maintenance a été signé avec les fournisseurs.	EGT	MT	2 800	2 800	0	0	2 800	1 400	0	1 400	4 200	établir et implanter
149	Gestion de la maintenance des équipements	Des mécanismes permettent de gérer la mise au rebut sécuritaire des équipements, incluant l'effacement des données confidentielles.	S	MT	560	0	0	0	0	280	0	280	280	établir processus
150	Gestion de la maintenance des systèmes	Des mécanismes formels de tests de performance des systèmes sont présents.	EGT	MT	1 400	1 400	0	0	1 400	840	0	840	2 240	établir processus
151	Gestion de la maintenance des systèmes	Un calendrier et un registre sont suivis indiquant les interventions relatives à la maintenance logicielle, la nature des modifications, le nom et la signature de l'intervenant.	EGT	MT	840	0	0	0	0	840	0	840	840	établir processus
152	Gestion de la maintenance des systèmes	La documentation technique et de maintenance, claire et à jour, de tous les systèmes est présente.	EGT	MT	840	560	0	0	560	840	0	840	1 400	établir processus
153	Identification des ressources à l'application	Un mécanisme formel encadre la gestion des codes d'accès. Un formulaire doit être signé par les personnes autorisées et qualifiées. (ISO 11.1.1)	D	MT	560	840	0	0	840	840	0	840	1 680	établir processus
154	Identification des ressources à l'application	La session d'un utilisateur est interrompue après une période d'inactivité d'une heure au maximum. *(Mesure du Cadre	D	MT	560	840	0	0	840	840	0	840	1 680	sensibiliser et documenter

					Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
		global no.26) (ISO 11.5.5)												
155	Identification des ressources à l'application	Pour les applications sensibles (cote d'intégrité ou de confidentialité de 4), une période de connexion maximale a été établie au-delà de laquelle les utilisateurs (ou les programmes en lot) doivent s'authentifier à nouveau. *(Mesure du CGGAI...	D	MT	1 400	11 200	0	0	11 200	840	0	840	12 040	vérifier et documenter
156	Identification des ressources à l'application	Des mécanismes enregistrent les événements importants (tentatives multiples infructueuses, modification des règles de gestion des codes d'accès) et une revue des journaux est effectuée périodiquement. *(Mesure du Cadre global no.29)	D	MT	2 800	8 400	0	0	8 400	1 400	0	1 400	9 800	établir et mettre en place
157	Identification des ressources à l'application	Une revue périodique des codes d'accès définis dans l'application est réalisée. Les codes d'accès n'ayant pas été utilisés depuis un an doivent être désactivés ou détruits. *(Mesure du Cadre global no.23) (ISO 11.2.4)	D	MT	1 400	0	0	0	0	560	0	560	560	établir processus
158	Identification des ressources à l'application	Une procédure est en place afin de détruire les codes d'accès lorsque la personne s'absente pour une période de plus de six semaines ou si elle quitte définitivement l'organisme. *(Mesure du Cadre global no.20) (ISO 11.2.1)	D	MT	560	840	0	0	840	560	0	560	1 400	établir processus
159	Gestion des mécanismes d'authentification à l'application	Des procédures assurent la qualité et la solidité du processus d'authentification des utilisateurs (spécifiant, par exemple, la longueur minimale des mots de passe, la fréquence de leurs changements, la durée de conservation de leur historique etc.…	D	MT	560	840	0	0	840	560	0	560	1 400	établir processus
160	Gestion des	En cas d'oubli du mot de passe,	D	MT	1 400	1 400	0	0	1 400	0	0	0	1 400	établir et implanter

					Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
	mécanismes d'authentification à l'application	l'identité de l'utilisateur est validée avant d'octroyer un nouveau mot de passe.												
161	Gestion des mécanismes d'authentification à l'application	La composition du mot de passe est-elle adéquate et obligatoire.*(Mesure du Cadre global no.28) (ISO 11.5.3) 8 caractères minimum - lettres, chiffres ou caractères spéciaux.	D	MT	1 400	1 400	0	0	1 400	0	0	0	1 400	vérifier et documenter
162	Gestion des mécanismes d'authentification à l'application	Le système garde un historique des dix derniers mots de passe. *(Mesure du Cadre global no.28)	D	MT	2 800	8 400	0	0	8 400	0	0	0	8 400	établir et implanter
163	Gestion des profils d'accès à l'application	Les profils d'accès sont révisés périodiquement permettant de suspendre, révoquer, bloquer ou radier les privilèges d'accès *(Mesure du Cadre global no.20) Un contrôle rigoureux est effectué sur le processus d'assignation, de modification et de retrait de droits d'accès. Un processus est présent pour la mise a jour du registre des droits d'accès lors du départ d'un membre du personnel ou lors d'un changement de fonction	D	MT	1 400	1 400	0	0	1 400	1 400	0	1 400	2 800	établir et implanter
164	Revue des journaux de sécurité et enquête pour l'application	Les journaux de sécurité des applications supportant chaque processus d'affaires ayant obtenu une cote 3 ou 4 pour les dimensions de disponibilité, d'intégrité ou de confidentialité sont vérifiés périodiquement. Les types d'événements devant être …	D	MT	2 800	0	0	0	0	2 800	0	2 800	2 800	établir et implanter
165	Gestion des applications supportant les processus	Une configuration standard et sécuritaire a été définie, documentée et est adéquatement appliquée à l'application. *(Mesure du Cadre global no.11):	D	MT	1 400	4 200	0	0	4 200	840	0	840	5 040	établir standard

# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
					Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
		Suppression de comptes génériques - Paramètres de contrôle des codes d'accès - …												
166	Gestion des applications supportant les processus	Les activités de l'administrateur de l'application sont journalisés et vérifiés périodiquement par une personne indépendante. (ISO 10.10.4)	D	MT	1 400	1 400	0	0	1 400	840	0	840	2 240	établir et implanter
167	Gestion des applications supportant les processus	Une revue périodique de l'application est effectuée afin de s'assurer de l'absence de nouvelles vulnérabilités. (ISO 15.2.2)	D	MT	1 400	1 400	0	0	1 400	0	0	0	1 400	établir processus
168	Gestion des codes d'accès à la base de données	Les mots de passe des comptes d'administrateurs de système sont modifiés à chaque 30 jour.	D	MT	1 400	1 400	0	0	1 400	840	0	840	2 240	établir et implanter
169	Documentation des schémas de la base de données	La documentation de la base de données a été effectuée et est à jour.	D	MT	1 400	4 200	0	0	4 200	840	0	840	5 040	établir et implanter
170	Sensibilisation et respects des exigences	Des outils permettent de contrôler l'intégrité des mises à jour de la base de données.	D	MT	0	0	0	0	0	0	0	0	0	
171	Ententes et relations avec les tiers	Un mécanisme est mis en place et vise à identifier les principaux risques de chaque fournisseur.	S	MT	0	0	0	0	0	0	0	0	0	
				Sous-total	**116 200**	**207 900**	**0**	**131 800**	**339 700**	**100 120**	**0**	**100 120**	**439 820**	

172	Budget et ressources allouées à la sécurité	L'organisme dispose de ressources humaines et financières pour gérer la sécurité et la PRP.	C	LT	0	38 220	0	5 000	43 220	0	0	0	43 220	Salaire annuel pour une personne qui gère la mise en œuvre du plan directeur de sécurité. Une prime de 5 % du salaire est rajoutée. La personne sera sollicitée pour cette action à 50 %. Le 50 % sera attribué aux autres actions de sécurité. 5000 $ pour la formation et

					Coûts non-récurrents					Coûts récurrents			Total ($)	Remarques / Commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
														le perfectionnement.
173	Journalisation et gestion des incidents pour l'application	Un système enregistre pour chaque incident les informations suivantes : date, heure, nature de l'incident, durée d'indisponibilité, le statut (en cours, en étude, résolu), les mesures correctives apportées, ainsi que le nom de l'intervenant.	D	LT	1 400	0	0	0	0	1 400	0	1 400	1 400	établir et implanter
174	Gestion des licences	Révision périodique de la présence de logiciels illégaux sur les postes de travail.	S	LT	1 400	1 400	0	0	1 400	1 400	0	1 400	2 800	Établir et implanter processus
175	Gestion des licences	Les copies originales des logiciels et progiciels sont conservés sous clé et ne sont accessibles qu'aux personnes autorisées. *(Mesure du Cadre global no.47)	S	LT	0	0	0	0	0	0	0	0	0	
				Sous-total	**2 800**	**39 620**	**0**	**5 000**	**44 620**	**2 800**	**0**	**2 800**	**47 420**	

☑ **Le taux horaire de 40 $ est celui d'un professionnel et inclut les avantages sociaux**

*** **Les ressources sollicitées sont : (EGT : Équipe de gestion technologique, S : Sécurité, D : Développement, C : Coordination)**

+ **CT : court terme, MT : moyen terme, LT : long terme.**

5.6. ANNEXE 3.C : PLAN DIRECTEUR DE LA SÉCURITÉ DE L'INFORMATION POUR LE TECHNOCENTRE

					Coûts non récurrents					Coûts récurrents			Total ($)	Remarques / commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT, R) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
1	Vision de la sécurité	L'établissement s'assure formellement que les utilisateurs ont pris connaissance de la politique.	S	CT	0	0	0	0	0	0	0	0	0	À inclure au processus d'embauche (RH)
2	Budget et ressources alloués à la sécurité	L'organisme dispose de ressources humaines et financières pour gérer la sécurité et la PRP.	C	CT	0	53508	0	5000	58508	0	0	0	58508	Salaire annuel pour une personne qui gère la mise en œuvre du plan directeur de sécurité. Une prime de 5 % du salaire est rajoutée. La personne sera sollicitée pour cette action à 70 %. Le 30 % sera attribué aux autres actions de sécurité. 5000 $ pour la formation et le perfectionnement.
3	Bilan annuel de la sécurité	Un rapport annuel de l'état du dossier de la sécurité de l'information est préparé.	S	CT	0	0	0	0	0	2800	0	2800	2800	70h/année
4	Gestion des accès aux locaux informatiques	Un registre de personnes autorisées à accéder aux locaux informatiques est utilisé consignant l'énumération des tâches autorisées pour chacune d'entre elles, et la durée habituelle de leur intervention.	S	CT	0	560	0	0	560	0	0	0	560	Exemple de registre = Imad fournira un pro-format
5	Contrôle de l'exploitation (production informatique)	Des procédures d'exploitation sont présentes pour les opérateurs et sont à jour.	ES	CT	0	0	0	15000	15000	22800	0	22800	37800	Outil d'ordonnancement de lots (15 000 $). Élaboration des procédures (500h). Révision des procédures (70h en récurrent)
6	Anti-codes malicieux pour les postes de travail	Les utilisateurs connaissent les procédures à suivre en cas d'incidents.	S	CT	0	0	0	0	0	560	0	560	560	Sensibilisation: 14h/année (récurrent)
7	Sauvegarde de sécurité des données et des systèmes présents sur les postes de travail	Dans le cas extraordinaire où des informations sensibles sont entreposées sur les postes de travail, des procédures de sauvegarde ont été rédigées pour les postes de travail	ES	CT	0	0	0	0	0	1400	0	1400	1400	Sensibilisation: proscrire l'utilisation des supports locaux sur poste ou portables (35h/année)

					Coûts non récurrents					Coûts récurrents			Total ($)	Remarques / commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT, R) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
		des utilisateurs et prévoit la sauvegarde périodique des données.												
8	Sauvegarde de sécurité des données et des systèmes présents sur les postes de travail	Ces procédures ont été distribuées aux utilisateurs.	S	CT	0	0	0	0	0	0	0	0	0	Sensibilisation: proscrire l'utilisation des supports locaux sur poste ou portables
9	Protection des portatifs	Par défaut, les données sensibles stockées dans des portatifs sont chiffrées.	ES	CT	0	0	0	0	0	0	0	0	0	Tous les disques durs des portables et postes de travail devraient être chiffrés
10	Protection des portatifs	Les utilisateurs sont sensibilisés à ne pas laisser sans surveillance leur portatif et à assurer leur protection.	S	CT	0	0	0	0	0	560	0	560	560	Sensibilisation: 14h/année (récurrent)
11	Intégration de la sécurité dans le développement et l'acquisition des S.I	La certification préalable par le MSSS est nécessaire pour les applications partageables inter sites par l'intermédiaire d'un réseau de télécommunication.	D	CT	0	4000	0	0	4000	560	0	560	4560	Processus Dév. Apps. + GMEP et GCHG. Révision du processus (14h en récurrent)
12	Activités de développement et d'acquisition des systèmes d'information)	Lorsque le développement d'application est confié à un fournisseur externe, le contrat de service exige le respect de ces normes et procédures.	D	CT	0	0	0	0	0	2800	0	2800	2800	processus Dév. Apps. + GMEP et GCHG. La MAJ/révision des contrats est récurrente
13	Gestion de la documentation (maintenance et développement informatique)	Une documentation par application est maintenue à jour et comporte les instructions d'exploitation, de sécurité, de reprise et d'intervention sur anomalie.	D	CT	0	0	0	0	0	0	0	0	0	processus Dév. Apps. + GMEP et GCHG
14	Contrôle des changements aux applications	Des mécanismes assurent le contrôle des changements sécuritaire des applications.	D	CT	0	8000	0	0	8000	1400	0	1400	9400	processus Dév. Apps. + GMEP et GCHG (200h). Révision et MAJ (35h en récurrent)
15	Contrôle des changements aux applications	Ces mécanismes requièrent la mise a jour de la documentation après modification.	D	CT	0	0	0	0	0	0	0	0	0	processus Dév. Apps. + GMEP et GCHG

					Coûts non récurrents					Coûts récurrents			Total ($)	Remarques / commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT, R) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
16	Programme de sensibilisation et de formation	Un programme a été élaboré pour sensibiliser le personnel à la sécurité des actifs informationnels de l'organisme et de la PRP.	S	CT	0	0	0	5000	5000	0	0	0	5000	Ce contrôle est couvert dans les 15 mesures obligatoires. Les coûts d'acquisition incluent des outils de sensibilisation tels que les "posters" ou d'autres types d'affiches.
17	Programme d'accueil des employés	Le programme d'accueil prévoit la présence d'éléments concernant la sécurité informatique et la PRP. (Signature d'un code d'éthique, l'explication de l'importance de la protection des renseignements pour l'organisme, remise de la politique de sécurité, et	S	CT	0	0	0	0	0	840	0	840	840	Mise à jour des documents du programme (21h en récurrent)
18	Architecture redondante et sécuritaire (réseau)	Une revue formelle est effectuée périodiquement afin d'identifier les vulnérabilités du réseau de l'organisme et des équipements de support (alimentation électrique, etc.).	ES	CT	0	0	0	0	0	2800	0	2800	2800	Rédaction/MAJ de procédures/directives (35h). Revue formelle des vulnérabilités 35h en récurrent).
19	Sécurité des réseaux internes	Une analyse est réalisée périodiquement sur la sensibilité et une évaluation formelle est faite périodiquement sur la perméabilité des différents segments du réseau interne et faire évoluer les dispositifs de sécurité en conséquence.	ER	CT	0	0	0	0	0	2800	0	2800	2800	Rédaction/MAJ de procédure/directive : 35h. Analyse des segments: 35h/année (récurrent)
20	Contrôle des accès aux réseaux	Toutes les créations ou modifications de codes d'accès ainsi que les changements aux dispositifs de sécurité réseau sont journalisées et analysées.	ER	CT	0	5600	0	0	5600	1400	0	1400	7000	Mise en place : 140h. Analyse des journaux : 35h/année (récurrent)

					Coûts non récurrents					Coûts récurrents			Total ($)	Remarques / commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT, R) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
21	Contrôle des accès aux réseaux	Des dispositifs permettent le déclenchement d'alarme associée à certains évènements (tentatives d'accès infructueuses).	ER	CT	0	4160	0	0	4160	0	0	0	4160	Outil de monitoring du genre Swatch (Unix) et Illuminate (Windows)
22	Revue des journaux de sécurité et enquête pour les réseaux	Un examen régulier est effectué par une personne désignée sur les journaux des composantes du réseau qui a été préalablement configuré pour enregistrer les événements de sécurité.	ER	CT	0	0	0	35000	35000	5560	0	5560	40560	Outil de centralisation des logs Windows (ex. MS-SMS). Rédaction de directive/procédure : 35h. Examen régulier des journaux: 2h/sem. ou 104/année
23	Protection de l'application de messagerie	Les utilisateurs sont sensibilisés à l'impact sur la performance des systèmes de messagerie de la transmission de chaînes de lettres Électroniques et autres types de courrier non sollicités.	ES	CT	0	0	0	0	0	0	0	0	0	Sensibilisation : 7h/année (inclut au plan de l'Agence)
24	Gestion des privilèges du personnel de support réseau	Les privilèges d'accès du personnel informatique aux ressources réseau sont limités et contrôlés.	ER	CT	0	2800	0	0	2800	1400	0	1400	4200	Mise en place de la mesure (70h). Rédaction/MAJ (35h récurrents)
25	Administration des équipements réseau	Un code d'accès unique a été attribué à chacun des administrateurs.	ER	CT	0	0	0	0	0	560	0	560	560	Faire auditer 1 fois/an
26	Administration des équipements réseau	Une revue formelle est effectuée périodiquement sur les paramètres de sécurité des équipements réseau et de télécommunication lors des mises en production.	ER	CT	0	0	0	0	0	2800	0	2800	2800	Rédaction de procédure/directive : 35h. Revue formelle des paramètres: 35h/année
27	Administration des équipements réseau	Un journal permet de consigner toutes les interventions de maintenance matérielle et logicielle, la nature des modifications, le nom et la signature de l'intervenant.	ER	CT	0	4800	0	0	4800	560	0	560	5360	ITIL: GCHG
28	Administration des équipements réseau	Le contrôle des accès aux ports de diagnostic et de configuration est adéquat.	ER	CT	0	0	0	0	0	560	0	560	560	

					Coûts non récurrents					Coûts récurrents			Total ($)	Remarques / commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT, R) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
29	Sauvegarde des configurations réseau	Les copies de sauvegarde (exécutables et paramètres de configuration) sont testés périodiquement.	ER	CT	0	0	0	0	0	5560	0	5560	5560	Rédaction de procédure/directive : 35h. Tests périodiques des copies de sauvegarde: 2h/semaine
30	Identification des ressources au serveur (contrôle des accès au serveur)	Chaque personne qui accède le serveur possède un code d'accès unique.	ES	CT	0	1400	0	0	1400	1400	0	1400	2800	Assignation de codes d'accès uniques
31	Identification des ressources au serveur (contrôle des accès au serveur)	Des dates d'expiration sont prévues pour le personnel temporaire.	ES	CT	0	0	0	0	0	0	0	0	0	
32	Identification des ressources au serveur (contrôle des accès au serveur)	Les événements importants sont journalisés et vérifiés (tentatives multiples infructueuses, modification des règles de gestion des codes d'accès).	ES	CT	0	5600	0	0	5600	14560	0	14560	20160	Mise en place de la journalisation : 140h. Vérification des journaux : 7h/semaine
33	Identification des ressources au serveur (contrôle des accès au serveur)	Une revue périodique des codes d'accès définis sur le serveur est réalisée. Les codes d'accès n'ayant pas été utilisés depuis un an doivent être désactivés ou détruits.	ES	CT	0	0	0	0	0	2800	0	2800	2800	Revue formelle des codes d'accès: 70/année
34	Gestion des profils d'accès pour le serveur	Toute création ou modification des règles d'authentification est journalisée dans un registre maintenu à jour.	ES	CT	0	560	0	0	560	0	0	0	560	ITIL: GCHG
35	Gestion des profils d'accès pour le serveur	Les profils d'accès sont révisés périodiquement permettant de suspendre, révoquer, bloquer ou radier les privilèges d'accès	ES	CT	0	0	0	0	0	0	0	0	0	Incluse dans la mesure 03.B.01.01.10
36	Gestion des profils d'accès pour le serveur	Des profils d'accès regroupent des rôles ou fonctions précises et régissent les autorisations d'accès aux systèmes. Ces profils ont été créés par les détenteurs. Les accès aux	ES	CT	0	5600	0	0	5600	1400	0	1400	7000	Mise en place du processus (140h). Révision (35h) Faire auditer 1 fois/an

# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT, R) +	Coûts non récurrents					Coûts récurrents			Total ($)	Remarques / commentaires
					Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
		services et aux transactions sont attribués selon les fonctions des personnes.												
37	Gestion des profils d'accès pour le serveur	Un contrôle rigoureux est effectué sur le processus d'assignation, de modification et de retrait de droits d'accès.	ES	CT	0	5600	0	0	5600	1400	0	1400	7000	Mise en place du processus (140h). Révision (35h) Faire auditer 1 fois/an
38	Journalisation et gestion des incidents au niveau du serveur	Des mesures et des analyses de performance sont effectuées régulièrement sur le serveur afin de faciliter la détection d'anomalies.	ES	CT	0	0	0	0	0	8320	0	8320	8320	Inclut à l'action #28+33 / ITIL: GCAP / Analyse périodique : 4h/semaine
39	Journalisation et gestion des incidents au niveau du serveur	Un système enregistre pour chaque incident les informations suivantes : date, heure, nature de l'incident, durée d'indisponibilité, le statut (en cours, en étude, résolu), les mesures correctives apportées, ainsi que le nom de l'intervenant.	ES	CT	0	0	0	0	0	2080	0	2080	2080	Inclut à l'action #28+33 / ITIL: GCAP / Analyse périodique : 1h/semaine
40	Revue des journaux de sécurité et enquête au niveau du serveur	Les journaux de sécurité des systèmes supportant chaque processus d'affaires ayant obtenu une cote 3 ou 4 pour les dimensions de disponibilité, d'intégrité ou de confidentialité sont vérifiés périodiquement. Les types d'événements devant être journalisés	ES	CT	0	0	0	0	0	10240	0	10240	10240	Vérification des journaux : 4h/sem. + audit externe 4h/mois
41	Revue des journaux de sécurité et enquête au niveau du serveur	Un examen régulier est effectué sur les journaux des composantes du serveur qui a été préalablement configuré pour enregistrer les	ES	CT	0	0	0		0	3480	0	3480	3480	Rédaction de directive/procédure : 35h, Vérification, Vérification: 1h/semaine

# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT, R) +	Coûts non récurrents					Coûts récurrents			Total ($)	Remarques / commentaires
					Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
		événements de sécurité.												
42	Gestion des serveurs	Une configuration standard et sécuritaire a été définie, documentée et est adéquatement appliquée au serveur : Suppression de comptes génériques - Paramètres de contrôle des codes d'accès - Paramètres de contrôle des mots de passe - Protection des fichier	ES	CT	0	11200	0	0	11200	2800	0	2800	14000	Révision et MAJ (récurrent)
43	Gestion des serveurs	Tous les services/ports superflus sont désactivés.	ES	CT	0	0	0	0	0	1400	0	1400	1400	35 en récurrent
44	Gestion des serveurs	Un audit périodique (entre autres des tests d'intrusion et des analyses de vulnérabilités) est effectué périodiquement.	ES	CT	0	0	0	0	0	3080	0	3080	3080	Préparation de l'audit : 70h. Audit: 7h/année
45	Gestion de la maintenance des équipements (serveurs)	Un calendrier de maintenance a été élaboré et tient compte de tous les équipements.	ES	CT	0	0	0	0	0	2800	0	2800	2800	Maintient et suivi du calendrier
46	Gestion de la maintenance des équipements (serveurs)	Des mécanismes permettent de gérer la mise au rebut sécuritaire des équipements, incluant l'effacement des données confidentielles	ES	CT	0	0	0	0	0	2800	0	2800	2800	Selon le volume, 70h/an. À attacher avec le processus de la gestion des actifs de l'Agence
47	Gestion de la maintenance des équipements (serveurs)	Un calendrier et un registre sont suivis indiquant les interventions relatives à la maintenance logicielle, la nature des modifications, le nom et la signature de l'intervenant.	ES	CT	0	2080	0	0	2080	0	0	0	2080	ITIL: GCHG
48	Gestion des profils d'accès à l'application	Toute création ou modification des règles d'authentification est journalisée dans un registre maintenu à jour.	D	CT	0	0	0	0	0	0	0	0	0	

					Coûts non récurrents					Coûts récurrents			Total ($)	Remarques / commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT, R) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
49	Gestion des profils d'accès à l'application	Les profils d'accès sont révisés périodiquement permettant de suspendre, révoquer, bloquer ou radier les privilèges d'accès.	D	CT	0	0	0	0	0	1400	0	1400	1400	Révision des profils d'accès: 35h/année
50	Gestion des profils d'accès à l'application	Un processus est présent pour la mise a jour du registre des droits d'accès lors du départ d'un membre du personnel ou lors d'un changement de fonction.	D	CT	0	0	0	0	0	0	0	0	0	Fait au niveau de l'Agence
51	Revue des journaux de sécurité et enquête pour l'application	Un examen régulier est effectué sur les journaux des composantes de l'application qui a été préalablement configuré pour enregistrer les événements de sécurité.	D	CT	0	0	0	0	0	560	0	560	560	35h/année
52	Copies de sécurité de la base de données	Les copies de sécurité sont révisées périodiquement.	ES	CT	0	0	0	0	0	11800	0	11800	11800	Rédaction de directive/procédure: 70h. Vérification des copies de sécurité : 7h/semaine
53	Contrôles de protection des données en lecture	Les options de menus et transactions de l'application permettant d'accéder en modification aux données des processus catégorisés 3 ou 4 sont attribuées à des personnes autorisées selon leurs fonctions.	D	CT	0	0	0	0	0	1400	0	1400	1400	Audit annuel
54	Ententes et relations avec les fournisseurs	Des engagements sont inclus dans les contrats relativement à la sécurité stipulant et respectent les standards en vigueur et les exigences ministérielles, régionales et locales. Ces engagements inclus notamment : Le respect de la confidentialité - …	S	CT	0	0	0	0	0	5600	0	5600	5600	Révision annuelle des ententes selon les changements survenus
				Sous-total	**0**	**115468**	**0**	**60000**	**175468**	**137040**	**0**	**137040**	**312508**	

# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT, R) +	Coûts non récurrents					Coûts récurrents			Total ($)	Remarques / commentaires
					Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
55	Budget et ressources alloués à la sécurité	L'organisme dispose de ressources humaines et financières pour gérer la sécurité et la PRP.	C	MT	0	38220	0	5000	43220	0	0	0	43220	Salaire annuel pour une personne qui gère la mise en œuvre du plan directeur de sécurité. Une prime de 5 % du salaire est rajoutée. La personne sera sollicitée pour cette action à 50 %. Le 50 % sera attribué aux autres actions de sécurité. 5000 $ pour la formation et le perfectionnement.
56	Documentation de la gestion de la sécurité	Un manuel de gestion opérationnelle de la sécurité contient l'ensemble des normes, des procédures et des formulaires utilisés.	S	MT	0	11200	0	0	11200	1400	0	1400	12600	Élaboration du manuel de gestion (280h). MAJ du manuel (35h en récurrent) À arrimer avec l'Agence
57	Documentation de la gestion de la sécurité	Des mécanismes permettent de protéger la confidentialité de toute information portant sur les processus et les mesures touchant la sécurité des actifs informationnels.	S	MT	0	280	0	0	280	2800	0	2800	3080	À arrimer avec l'Agence
58	Gestion des accès aux locaux informatiques	Les accès temporaires sont correctement gérés (attribution, retrait et journalisation des accès).	S	MT	0	0	0	0	0	1400	0	1400	1400	Se fait au niveau de l'Agence,
59	Mécanismes de protection des documents électroniques qui transigent sur courrier électronique	Des mécanismes permettant le chiffrement des documents Électroniques qui ont été catégorisés 3 ou 4 pour les dimensions de confidentialité ou d'intégrité sont appliqués lorsque ces documents sont acheminés à l'extérieur du RTSS par courrier Électronique.	ES	MT	0	0	0	0	0	560	0	560	560	Audit annuel
60	Mécanismes de protection des documents électroniques qui transigent sur courrier électronique	Une procédure écrite est communiquée à cette fin aux utilisateurs pour leur permettre de s'y conformer.	ES	MT	0	0	0		0	0	0	0	0	Inclus dans la mesure 01.B.01.11.01

					Coûts non récurrents					Coûts récurrents			Total ($)	Remarques / commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT, R) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
61	Privilèges du personnel informatique	L'accès aux outils et utilitaires d'administration des systèmes d'exploitation est contrôlé par des mécanismes documentés.	S	MT	0	0	0	0	0	1400	0	1400	1400	À arrimer avec l'Agence
62	Contrôle de l'exploitation (production informatique)	Un calendrier des tâches à effectuer (cédule de production) est préparé en fonction des besoins définis par le détenteur de l'établissement.	ES	MT	0	0	0	0	0	0	0	0	0	
63	Contrôle de l'exploitation (production informatique)	Les activités effectuées par les opérateurs sont journalisées et révisées périodiquement.	ES	MT	0	0	0		0	5560	0	5560	5560	Rédaction de procédure/directive : 70h. Vérification des journaux : 2h/semaine
64	Mise au rebut des équipements et des supports magnétiques	Les contrats avec les fournisseurs prévoient des clauses spécifiques à cette fin. L'établissement s'assure du respect de ces clauses périodiquement.	S	MT	0	0	0	0	0	2800	0	2800	2800	Rédaction de directive/procédure: 35h. Révision des contrats : 35h/année
65	Haute disponibilité et redondance	Des mécanismes assurent la haute disponibilité et la redondance pour les processus dont la cote de disponibilité a été établie à 4.	ES	MT	0	16000	0	100000	116000	5600	0	5600	121600	Enveloppe de 100k$ pour compléter l'analyse de besoin d'architecture pour les dossiers D = 4 non encore identifiés en hébergement au TCR
66	Performance du serveur	Pour les processus d'affaires catégorisés 3 ou 4 sur la dimension de la disponibilité, des mécanismes permettent de surveiller la performance du serveur et l'utilisation des ressources afin d'en prévoir la saturation.	ES	MT	0	11200	0	70000	81200	0	0	0	81200	ITIL: GCAP + outils de collecte de données sur l'utilisation ress. Techno.
67	Gestion de la documentation (maintenance et développent informatique)	Des mécanismes permettent de gérer la documentation.	D	MT	0	5600	0	20000	25600	0	0	0	25600	ITIL: GMEP + GCHG. Outil de gestion documentaire

					Coûts non récurrents					Coûts récurrents			Total ($)	Remarques / commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT, R) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
68	Maintenance des applications achetées et supportées par les fournisseurs externes	Des mécanismes permettent de gérer les versions sources des applications obtenues des fournisseurs (ou ces dernières sont placées en fiducie)	D	MT	0	1400	0		1400	0	0	0	1400	À arrimer avec l'Agence
69	Contrôle des accès aux réseaux	Des mécanismes contrôlent les accès au réseau pour les connexions TCP/IP au réseau de l'organisme (pare-feu, routeur, etc.). Mesure du CGGAI no.55) Ces mécanismes permettent de protéger le réseau interne de l'Internet et la configuration de ceux-ci respec	ER	MT	0	2800	0	20000	22800	4200	0	4200	27000	À arrimer avec l'Agence
70	Journalisation et gestion des incidents pour les réseaux	Des mécanismes encadrent la journalisation systématique des tentatives d'accès infructueuses pour tous les équipements réseau.	ER	MT	0	0	0	0	0	0	0	0	0	Évolution à l'action #28+33 / ITIL: GCAP / Analyse périodique : 1h/semaine
71	Revue des journaux de sécurité et enquête pour les réseaux	Des mécanismes permettent d'effectuer une vérification et des enquêtes en cas de détection d'anomalie. Un processus d'escalade est en place à cette fin.	ER	MT	0	0	0	0	0	2800	0	2800	2800	À arrimer avec l'Agence
72	Gestion des privilèges du personnel de support réseau	Des mécanismes contrôlent les modifications ou les ajouts d'outils et utilitaires d'administration réseau.	ER	MT	0	0	0	0	0	2800	0	2800	2800	ITIL: GCHG (évolution)
73	Contrôle de la mise en place des systèmes d'exploitation	Une évaluation formelle des spécifications de sécurité du système d'exploitation est effectuée précédant leur mise en place ou présence d'un guide de configuration.	ES	MT	0	5600	0	0	5600	2800	0	2800	8400	Élaboration du guide + révision périodique

# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT, R) +	Coûts non récurrents					Coûts récurrents			Total ($)	Remarques / commentaires
					Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
74	Contrôle de la mise en place des systèmes d'exploitation	Des mécanismes permettent des tests d'acceptation et des tests de performance si un nouveau système d'exploitation est mis en place.	ES	MT	0	5600	0	10000	15600	0	0	0	15600	Mise en place d'environnements contrôlés
75	Contrôle de la mise en place des systèmes d'exploitation	Une vérification systématique de la configuration de sécurité du système d'exploitation est effectuée suite à une nouvelle installation ou à une mise à niveau majeure.	ES	MT	0	2800	0	0	2800	0	0	0	2800	ITIL: GMEP (évolution)
76	Gestion de la maintenance des systèmes (serveurs)	Des mécanismes formels de tests de performance des systèmes sont présents.	ES	MT	0	5600	0	0	5600	1400	0	1400	7000	Mise en place des mécanismes (140h). Révision des mécanismes (35h)
77	Gestion des mécanismes d'authentification à l'application	Les mots de passe doivent être conformes aux exigences minimales du CGGAI/volet sécurité	D	MT	0	1400	0	0	1400	0	0	0	1400	Suivi avec les fournisseurs d'application
78	Gestion des mécanismes d'authentification à la base de données	Des procédures assurent la qualité et la solidité du processus d'authentification à la base de données (spécifiant, par exemple, la longueur minimale des mots de passe, la fréquence de leurs changements, la durée de conservation de leur historique etc.).	D	MT	0	5600	0	0	5600	1400	0	1400	7000	Mise en place des mécanismes (140h). Révision des mécanismes (35h)
79	Journalisation et gestion des incidents au niveau de la base de données	Des mécanismes encadrent la journalisation systématique des tentatives d'accès infructueuses pour la base de données.	D	MT	0	5600	0	0	5600	1400	0	1400	7000	Mise en place des mécanismes (140h). Révision des outils et du processus
80	Revue des journaux de sécurité et enquête au niveau de la base de données	Les journaux de sécurité des systèmes supportant chaque processus d'affaires ayant obtenu une cote 3 ou 4 pour les dimensions de disponibilité, d'intégrité ou de confidentialité sont	D	MT	0	0	0	0	0	3320	0	3320	3320	Rédaction/MAJ de procédure/directive : 35h. Vérification des journaux : 4h/mois

# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT, R) +	Coûts non récurrents					Coûts récurrents			Total ($)	Remarques / commentaires
					Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
		vérifiés périodiquement. Les types d'événements devant être journalisés												
81	Gestion de la base de données supportant les processus	Les changements apportés à la configuration de la base de données sont journalisés et contrôlés.	D	MT	0	1400	0	0	1400	1400	0	1400	2800	Mise en place de la directive (35h). Suivi avec les fournisseurs d'application (35 en récurrent)
82	Documentation et schéma de la base de données	La documentation de la base de données a été effectuée et est à jour.	D	MT	0	5600	0	0	5600	1400	0	1400	7000	Mise en place de la directive (140h). Suivi avec les fournisseurs d'application (35 en récurrent)
83	Documentation et schéma de la base de données	Les appels d'offre spécifient les critères de documentation de la base de données.	D	MT	0	1400	0	0	1400	280	0	280	1680	Rédaction de la directive (35h). MAJ de la directive (7h en récurrence)
84	Contrôles de chiffrement des tables de données	Des mécanismes de chiffrement sont définis pour le processus si celui-ci requiert l'entreposage de documents hautement confidentiels (catégorisés à un niveau de 4).	D	MT	0	5600	0	0	5600	1400	0	1400	7000	Définir les mécanismes et l'étendu de leur application.
85	Contrôles de protection des données en lecture	Les tables et fichiers sont adéquatement protégés en écriture pour les processus catégorisés 3 ou 4 sur la dimension confidentialité. Uniquement les codes d'accès autorisés peuvent accéder les données.	D	MT	0	0	0	0	0	0	0	0	0	Suivi avec les fournisseurs d'application
86	Ententes et relations avec les fournisseurs	Un mécanisme formel a été mis en place afin de régir le choix des tiers et leurs relations.	S	MT	0	5600	0	0	5600	1400	0	1400	7000	Mise en place du mécanisme (140h). MAJ (35h en récurrent). À arrimer avec l'Agence
				Sous-total	**0**	**138500**	**0**	**225000**	**363500**	**47520**	**0**	**47520**	**411020**	

					Coûts non récurrents					Coûts récurrents			Total ($)	Remarques / commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT, R) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
87	Budget et ressources alloués à la sécurité	L'organisme dispose de ressources humaines et financières pour gérer la sécurité et la PRP.	C	LT	0	38220	0	5000	43220	0	0	0	43220	Salaire annuel pour une personne qui gère la mise en œuvre du plan directeur de sécurité. Une prime de 5 % du salaire est rajoutée. La personne sera sollicitée pour cette action à 50 %. Le 50 % sera attribué aux autres actions de sécurité. 5000 $ pour la formation et le perfectionnement.
88	Gestion des profils d'accès pour le serveur	Des profils d'accès regroupent des rôles ou fonctions précises et régissent les autorisations d'accès aux systèmes. Ces profils ont été créés par les détenteurs. Les accès aux services et aux transactions sont attribués selon les fonctions des personnes.	ES	LT	0	2800	0	0	2800	1400	0	1400	4200	
89	Revue des journaux de sécurité et enquête pour l'application	Des mécanismes permettent d'effectuer une vérification et des enquêtes en cas de détection d'anomalie.	D	LT	0	5600	0	0	5600	1400	0	1400	7000	Suivi avec les fournisseurs d'application
90	Interconnexion entre les applications	Des mécanismes de contrôle ont été mis en place afin de protéger l'information lors d'échange d'information entre l'application et un système d'information.	D	LT	0	7000	0	0	7000	1400	0	1400	8400	Validation des schémas et des interdépendances
91	Gestion de la base de données supportant les processus	Une configuration standard et sécuritaire a été définie, documentée et est adéquatement appliquée à la base de données. Suppression de comptes génériques - Fermeture de ports non requis et non sécuritaire - Paramètres de contrôle des codes d'accès - …	D	LT	0	5600	0	0	5600	1400	0	1400	7000	À arrimer avec l'Agence

					Coûts non récurrents					Coûts récurrents			Total ($)	Remarques / commentaires
# Action	Objectif du contrôle	Description de l'action	Ressources sollicitées ***	Type d'action (CT, MT, LT, R) +	Coûts des ressources internes absorbés ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Coûts d'acquisition ($)	Sous-total ($)	Coûts des ressources internes supplém. ($)	Coûts des ressources externes ($)	Sous-total ($)		
92	Ententes et relations avec les fournisseurs	Les procédures de choix des tiers incluent une mesure d'analyse de risque et une évaluation des contrôles exercés par les tiers.	S	LT	0	0	0	0	0	0	0	0	0	Inclus dans la mesure 04.A.02.01.02
				Sous-total	**0**	**59220**	**0**	**5000**	**64220**	**5600**	**0**	**5600**	**69820**	

☑ **Le taux horaire de 40 $ est celui d'un professionnel et inclut les avantages sociaux**

*** **Les ressources sollicitées sont : (ES : Exploitation systèmes, ER : Exploitation réseaux, S : Sécurité, D : Développement, C : Coordination)**

+ **CT : court terme, MT : moyen terme, LT : long terme.**

Annexe 4 : Recommandation suite à l'audit interne

Agence de la santé
et des services sociaux
de Montréal
Québec

Recommandations suite à l'audit interne croisé réalisé sur les sites de l'Agence de Montréal, le 22 et 23 mars 2011

Recommandations	Direction de la santé publique	3725 St-Denis	Technocentre de Montréal
1	Installer l'antivirus sur les serveurs SQL et les inclure dans le processus de mise à jour.	Les tests de recouvrement du système Unix ne se font pas de façon régulière. Il faut uniformiser la situation afin de s'assurer que les données sauvegardées ne soient pas corrompues.	Sensibiliser le staff TI face à leurs rôles et responsabilités en relation à la sécurité des actifs informationnels.
2	Augmenter la longueur des mots de passe à 8 caractères et complexifier la composition de ces derniers.	Les poubelles et boites de carton doivent être proscrites dans les salles de serveurs, Il serait préférable d'utiliser une poubelle durant le déballage et la remettre à l'extérieure une fois le travail terminé.	Accroître la sécurité des médias dans le transport et la réception entre les divers sites.
3	Identifier le log du système d'exploitation afin de repérer les tentatives d'accès infructueuses et non autorisées.	Acquérir un classeur protégé et résistant au feu afin d'entreposer les contrats, documents importants et média.	Sécuriser la conservation des médias en cas de catastrophe.
4	Installer des gicleurs ainsi que des détecteurs de fumée dans la salle des serveurs.	Remplacer le registre papier dans la salle des serveurs par un système à carte magnétique pour plus d'imputabilité	Mettre en place une validation plus rigoureuse des tests de recouvrement.

5	Remplacer le registre papier dans la salle serveurs par un système à carte magnétique pour plus d'imputabilité.	Installer une caméra dans la salle des serveurs pour la visualisation et la détection à distance.	Avoir un processus clair et bien défini dans l'installation des logiciels sur les postes de travail.
6			Revoir périodiquement les divers logs pour la détection de problèmes ou d'autres irrégularités
7			Faire une maintenance plus rigoureuse de la gestion des accès.

Annexe 5 : Acronymes et définitions

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.
DGA	Direction générale adjointe
DIC	Disponibilité, Intégrité et Confidentialité (les 3 principes fondamentaux en sécurité de l'information)
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 de Montréal

Agence de la santé
et des services sociaux
de Montréal

Québec

Bilan de la sécurité des actifs informationnels 2005-2011