Procédure nº : POL-DG-123	**Date d'émission : 2006-06-15**
Titre : Politique de sécurité des actifs informationnels	**Date de révision : 2022-02-02**

Source : Direction générale

Responsable de l'application : Directrice des ressources financières et informationnelles

Destinataires : Conseil d'administration
Les gestionnaires et le personnel, incluant le personnel d'agence, de la Résidence, du Centre de jour et des Résidences Le 1615 et Le 1625
Les résidents, les aînés du Centre du jour et les locataires des Résidences Le 1615 et Le 1625 ainsi que leurs proches
Les bénévoles
Les stagiaires
Les contractuels et les partenaires

1. Préambule

L'établissement reconnaît que l'information 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. L'établissement reconnaît détenir, en outre, des renseignements personnels ainsi que des informations qui ont une valeur légale, administrative ou économique.

De plus, plusieurs lois et directives encadrent et régissent l'utilisation de l'information. L'établissement est assujetti à ces lois et doit s'assurer du respect de celles-ci.

En conséquence, l'établissement met en place la présente politique de sécurité des actifs informationnels qui oriente et détermine l'utilisation appropriée et sécuritaire de l'information et des technologies de l'information.

Un actif informationnel est une banque d'information électronique, un système d'information, un réseau de télécommunications, une infrastructure technologique, ou un ensemble de ces éléments ainsi qu'une composante informatique d'un équipement médical spécialisé ou ultraspécialisé.

(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.

2. Objectifs

- Assurer la disponibilité, l'intégrité, la confidentialité, l'authentification et l'irrévocabilité à l'égard de l'utilisation des réseaux informatiques, du réseau intégré de télécommunication multimédia (RITM) et de l'utilisation des actifs informationnels et des données corporatives;

- Assurer le respect de la vie privée des individus, notamment, la confidentialité des renseignements à caractère nominatif relatifs aux utilisateurs, à la clientèle et au personnel du réseau sociosanitaire;

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

3. Champ d'application

- La présente politique s'applique à l'ensemble du personnel de l'établissement. De plus, elle s'étend à toute personne physique ou morale qui utilise ou qui accède pour le compte de l'établissement, ou non, à des informations confidentielles, ou non, quel que soit le support sur lequel elles sont conservées.

- La présente politique s'applique à l'ensemble des actifs informationnels ainsi qu'à leur utilisation au sein de l'établissement, tels que les banques d'information électronique, les informations et les données sans égard aux médiums de support (fixe ou portable), les réseaux, les systèmes d'information, les logiciels, les équipements informatiques ou centres de traitement utilisés par l'établissement.

- La présente politique s'applique à l'ensemble des activités de collecte, d'enregistrement, de traitement, de garde et de diffusion des actifs informationnels de l'établissement.

4. Politique

- Toute personne au sein de l'établissement ayant accès aux actifs informationnels assume des responsabilités spécifiques en matière de sécurité et est redevable de ses actions auprès de la direction de l'établissement.

- 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.

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

- Les mesures de protection des actifs informationnels doivent permettre de respecter les prescriptions du Cadre global de gestion des actifs informationnels appartenant aux

établissements du réseau de la santé et des services sociaux – Volet sur la sécurité, de même que les lois existantes en matière d'accès, de diffusion et de transmission d'informations, et les obligations contractuelles de l'établissement de même que l'application des règles de gestion interne.

- Les actifs informationnels doivent faire l'objet d'une identification et d'une classification, idéalement à tous les quatre ans.

- Une évaluation périodique, en rotation par secteurs d'activités, 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.

- 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'établissement.

- Un programme continu de sensibilisation et de formation à la sécurité informatique doit être mis en place à l'intention du personnel de l'établissement.

- L'accès aux renseignements personnels des utilisateurs par le personnel de l'établissement doit être autorisé et contrôlé. Chaque système doit prévoir des droits d'accès différents selon les fonctions et responsabilités du personnel.

- Les renseignements personnels ne doivent être utilisés et ne servir qu'aux fins pour lesquels ils ont été recueillis ou obtenus.

- 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. Les détenteurs de système et le service informatique applique la politique sur le contrôle des accès aux actifs informationnels (POL-PRO-DRFI-554) en vigueur dans l'établissement.

- Les ententes et contrats dont l'établissement fait partie doivent contenir des dispositions garantissant le respect des exigences en matière de sécurité et de protection de l'information.

5. Responsabilité des personnes œuvrant dans l'établissement

- La directrice générale de l'établissement a désigné la directrice des ressources financières et informationnelles comme responsable de l'application de la présente politique.

- L'établissement exige de toute personne, qui utilise les actifs informationnels de l'établissement ou qui a/aura 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. Dès l'embauche, ces personnes s'engagent à respecter la présente politique en signant l'annexe 1 « Engagement à la confidentialité, au respect de la sécurité des actifs informationnels et aux principes d'utilisations des médias sociaux » retrouvée en annexe 1 de la politique sur la confidentialité de l'établissement (POL-DG-110).

- Le non-respect des obligations en lien avec la sécurité des actifs informationnels peut entraîner des mesures disciplinaires pouvant aller jusqu'au congédiement.

6. Rôles et responsabilités

6.1 Le conseil d'administration de l'établissement

Le conseil d'administration de l'établissement doit approuver la présente politique, s'assurer de sa mise en œuvre et faire le suivi de son application. À cet égard, il autorise et approuve la politique de sécurité des actifs informationnels, le plan directeur informatique et les plans de continuité des activités liées à ce secteur.

6.2 La directrice générale

La directrice générale est la première responsable de la sécurité des actifs informationnels au sein de l'établissement. Elle s'assure que les valeurs et les orientations en matière de sécurité soient partagées par l'ensemble des gestionnaires et du personnel de l'établissement. À cette fin, elle s'assure de l'application de la politique dans l'organisation, autorise les appuis financiers et logistiques nécessaires pour la mise en œuvre et l'application de la présente politique; soumets le bilan annuel concernant l'application de la politique au conseil d'administration par l'intermédiaire d'indicateurs au tableau de bord et du rapport annuel de la DRFI, exerce son pouvoir d'enquête et applique les sanctions prévues à la présente politique, lorsque nécessaire.

Pour la représenter en cette matière dans l'organisation et pour la réalisation de l'ensemble des mesures précitées, elle nomme un responsable de la sécurité des actifs informationnels.

6.3 La responsable de la sécurité informationnelle (RSI)

Le rôle de RSI est assumé par la directrice des ressources financières et informationnelles. À titre de représentante déléguée de la directrice générale en matière de sécurité des actifs informationnels, la RSI gère et coordonne la sécurité informationnelle au sein de l'établissement. Elle doit donc harmoniser l'action des divers acteurs dans l'élaboration, la mise en place, le suivi et l'évaluation de la sécurité de l'information. Cette responsabilité exige une vision globale de la sécurité informationnelle au sein de l'établissement.

La responsable de la sécurité des actifs informationnels veille à l'élaboration et à l'application de la politique sur la sécurité adoptée par l'établissement. Dans cette perspective, elle collabore avec tous les gestionnaires. Plus précisément, la responsable de la sécurité de l'établissement :

- élabore la politique sur la sécurité des actifs informationnels qui sera adoptée par l'établissement et soumet cette politique à la directrice générale et au conseil d'administration de l'établissement pour approbation;
- coordonne, avec les secteurs visés et en concordance avec les orientations régionales, la mise en œuvre de la politique sur la sécurité informationnelle adoptée par l'établissement et en suit l'évolution;
- identifie, en collaboration avec les gestionnaires, les détenteurs d'actifs informationnels dans leur secteur respectif;
- s'informe des besoins en matière de sécurité informationnelle auprès des détenteurs et des gestionnaires, leur propose des solutions et coordonne la mise en place de ces solutions;
- gère les aspects relatifs à l'escalade des incidents de sécurité informationnelle à l'échelle locale et procède à des évaluations de la situation en matière de sécurité;

- collabore avec la conseillère à la gestion des risques et à la qualité;

- s'assure de la mise en œuvre de toute recommandation découlant d'une vérification ou d'un audit. Elle s'assure également de l'application de la politique et procédure sur les audits sur la sécurité de l'information (POL-PRO-DRFI-556) en vigueur dans l'établissement;

- s'assure de l'application de la politique et procédure sur la gestion des incidents informatiques (POL-PRO-DRFI-555) en vigueur dans l'établissement;

- s'assure de l'application de la politique et procédure sur le contrôle des accès aux actifs informationnels (POL-PRO-DRFI-554) en vigueur dans l'établissement;

- produit au besoin, les bilans et les rapports relatifs à la sécurité des actifs informationnels appartenant à l'établissement en s'assurant que l'information sensible à diffusion restreinte est traitée de manière confidentielle et, après approbation de la directrice générale et du conseil d'administration, les soumet au coordonnateur régional de la sécurité des actifs informationnels.

6.4 Les détenteurs d'actifs informationnels

- assurent la sécurité d'un ou de plusieurs actifs informationnels, qu'ils leur soient confiés par le sous-ministre, la direction de l'établissement ou un tiers mandaté;

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

- s'assurent d'appliquer les recommandations émises suite à la tenue d'un audit sur la sécurité de l'information;

- s'assurent 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;

- déterminent les règles d'accès aux actifs dont ils assument la responsabilité avec l'appui du responsable de la sécurité informationnelle de l'établissement.

6.5 Le responsable de la protection des renseignements personnels (RPRP)

La directrice générale assume le rôle de RPRP. À titre de responsable de l'application de la Loi sur l'accès aux documents des établissements publics et sur la protection des renseignements personnels, la RPRP a un rôle de conseillère et/ou de valideur - approbateur auprès de la responsable de la sécurité des actifs informationnels 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 établissements publics et sur la protection des renseignements personnels. Cette responsabilité se manifeste aussi dès le début d'un développement d'un nouveau système où la RPRP doit introduire les préoccupations et les exigences relatives à la protection des renseignements nominatifs.

6.6 Utilisateur

Chaque membre du personnel utilisateur est responsable de respecter la présente politique, les normes, directives et procédures en vigueur en matière de sécurité des actifs

informationnels et d'informer son responsable de toute violation des mesures de sécurité dont il pourrait être témoin ou de toutes anomalies décelées pouvant nuire à la protection des actifs informationnels.

6.7 Le professionnel en sécurité de l'information (PSI)

Ce rôle est assumé par le responsable de l'informatique. Le rôle du professionnel de la sécurité de l'information est de conseiller la RSI sur les aspects technologiques et méthodologiques concernant la sécurité. Il coordonne les travaux reliés à l'implantation et aux contrôles des mesures de sécurité. Il coordonne et/ou réalise les tâches de sécurité opérationnelles qui lui sont confiées par la RSI.

6.8 Le gestionnaire

Le gestionnaire s'assure que tous ses employés sont au fait de leurs obligations découlant de la présente politique. Il les informe précisément des normes, directives et procédures de sécurité en vigueur.

Il informe et sensibilise son personnel à l'importance des enjeux de sécurité. Il doit s'assurer que les moyens de sécurité sont utilisés de façon à protéger effectivement l'information utilisée par son personnel.

Il communique au RSI tout problème d'importance en matière de sécurité de l'information.

6.9 Pilotes de systèmes nommés par le détenteur de l'actif informationnel

Les pilotes des systèmes ont la responsabilité d'assurer le fonctionnement sécuritaire d'un actif informationnel dès sa mise en exploitation, de contrôler et d'autoriser l'accès logique à tout actif informationnel dont ils ont la responsabilité d'utilisation. Les pilotes doivent également informer les utilisateurs de leurs obligations face à l'utilisation des systèmes d'information dont ils sont responsables lors de l'attribution et/ou le retrait des accès. Il procède également à l'évaluation du système pour lequel il est pilote ou détenteur en se référant à la politique et procédure sur les audits liés à la sécurité de l'information (POL-PRO-DRFI-556).

6.10 Le service informatique

Le rôle du service informatique à l'égard de la sécurité de l'information est d'agir en tant que fournisseur de service. Il fournit et maintient en état les moyens techniques de sécurité et s'assure de leur conformité aux besoins de sécurité déterminés par le détenteur. Ce rôle trouve son complément dans l'assistance et le conseil en vue d'une meilleure utilisation de ces moyens.

6.11 Direction des ressources humaines, techniques et alimentaires

La direction des ressources humaines, techniques et alimentaires est responsable d'informer tout nouvel employé de ses obligations découlant de la présente politique en vigueur dans l'établissement en lui remettant un résumé de la politique (Annexe 1).

6.12 Comité de sécurité des actifs informationnels (CAI)

Ce rôle est assumé par le comité de direction, auquel s'ajoute le responsable du service informatique qui est le professionnel en sécurité de l'information (PSI) et lorsque nécessaire la conseillère à la gestion des risques et à la qualité.

Le Comité joue avant tout un rôle-conseil auprès de la responsable de la sécurité informationnelle (RSI). Il 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, la mise en œuvre et la mise à jour des

mesures prévues au plan directeur. Il est aussi en mesure d'évaluer les incidences sur la sécurité de l'organisation que les nouveaux projets pourraient avoir.

7. Plan d'action de la sécurité des actifs informationnels

L'établissement élabore un plan d'action entériné par le comité de direction et le conseil d'administration et en fait le suivi.

8. Indicateurs

L'établissement cible annuellement des indicateurs de gestion en lien avec la sécurité informationnelle qui sont présentés au tableau de bord. Le comité de direction en assure le suivi.

9. Références

Principales lois, règlements, directives et autres références encadrant la présente politique :

- Le Cadre global sur la sécurité des actifs informationnels du réseau de la santé et des services sociaux – Volet sur la sécurité (ministère de la Santé et des services sociaux, octobre 2021);
- Architecture gouvernementale de la sécurité de l'information (février 2013);
- Charte des droits et libertés de la personne (L.R.Q., c.C-12);
- Charte canadienne des droits et libertés (1982, c. 11);
- Directive sur la sécurité de l'information et des échanges électroniques dans l'administration gouvernementale (février 2000);
- Directive sur le traitement et la destruction de tout renseignement, registre, donnée, logiciel, système d'exploitation ou autre bien protégé par un droit d'auteur, emmagasiné sur un équipement micro-informatique ou un support amovible (octobre 1999);
- Loi sur les archives (L.R.Q., ch. A-21.1);
- Loi sur l'accès aux documents des établissements publics et sur la protection des renseignements personnels (L.R.Q., ch. A-2.1);
- Loi sur l'administration publique (L.R.Q., A-6.011);
- Loi concernant le cadre juridique des technologies de l'information (L.R.Q., C-1.1);
- Certaines dispositions pertinentes du Code civil du Québec (C.C.Q);
- Certains articles du Code criminel du Canada (C.C.C);
- Loi sur la protection des renseignements personnels (L.R.C. (1985) ch. P-21);

- Loi sur la protection des renseignements personnels numériques (S-4, juin 2015);
- Loi canadienne sur le droit d'auteur (L.R. 1985, ch. C-42);
- Loi sur la propriété intellectuelle et les marques de commerce (L.R. 1985 ch. T-13);
- Normes en matière d'acquisition, d'utilisation et de gestion des droits d'auteur des documents détenus par le gouvernement et les ministères et établissements désignés (novembre 2000).

Signé le 2 février 2022 par
Date
Chantal Bernatchez
Directrice générale

Adopté par le conseil d'administration 8 février 2022 par
Date
Secrétaire du conseil d'administration

No de résolution : CA 22.09

Résumé de la politique Sécurité des actifs informationnels

Cette politique s'applique à **l'ensemble du personnel** de l'établissement **pour l'ensemble des actifs informationnels** (document papier, électronique ou imprimé de document électronique).

Les objectifs sont d'assurer la **disponibilité**, l'**intégrité,** la **confidentialité**, l'**authentification** et l'**irrévocabilité** (attribution à une personne de l'accès aux données d'un résident) à l'égard de l'utilisation des actifs informationnels, d'assurer le respect de la vie privée des individus et d'assurer la conformité aux lois et règlements.

Il s'agit d'une approche **globale et intégrée** qui tient compte des aspects humains, organisationnels, financiers, juridiques et techniques.

On se doit de respecter les prescriptions du **Cadre global de gestion des actifs informationnels du réseau de la santé et des services sociaux.**

Un programme continu de **sensibilisation** et de **formation** à la sécurité doit être mis en place.

L'accès aux renseignements personnels par le personnel doit être **autorisé** et **contrôlé** et être strictement utilisé pour l'exécution de ses tâches.

Rôles et responsabilités

Tous les employés : l'établissement exige de tout employé de se conformer aux dispositions de la politique de sécurité des actifs informationnels (POL PRO-DG-123).

Le conseil d'administration doit approuver la politique de sécurité et s'assurer de sa mise en œuvre et faire le suivi de son application.

La directrice générale est la première responsable de la sécurité des actifs informationnels au sein de l'établissement ainsi que la responsable des renseignements personnels (RPRP).

La responsable de la sécurité informationnelle (RSI) est la directrice des ressources financières et informationnelles. Déléguée par la directrice générale, elle gère et coordonne la sécurité informationnelle au sein de l'établissement.

Les détenteurs d'actifs informationnels assurent la sécurité **d'un ou de plusieurs** actifs informationnels dont ils assument la responsabilité.

L'utilisateur doit informer son responsable de toute violation des mesures de sécurité dont il pourrait être témoin ou de toutes anomalies décelées pouvant nuire à la protection des actifs informationnels.

Le professionnel en sécurité de l'information **(PSI)** est le responsable de l'informatique, qui joue un rôle de conseiller pour la responsable de la sécurité informationnelle (RSI).

Le gestionnaire s'assure de l'application de la politique de sécurité. Il informe et sensibilise son personnel à l'importance des enjeux de sécurité. Il communique au RSI tout problème d'importance. Il s'avère être souvent le détenteur d'actifs informationnels.

Le pilote de système assure le fonctionnement sécuritaire d'un actif informationnel.

Le service informatique est le fournisseur de service en terme de sécurité informationnelle. Il assiste et conseille les intervenants.

La direction des ressources humaines, techniques et alimentaires est responsable de remettre le résumé de la politique sur la sécurité des actifs informationnels à tout nouvel employé.

Le comité de sécurité des actifs informationnels (CAI) est assumé par le comité de direction et constitue un mécanisme de coordination et de concertation.