PO-18-001	**Politique sur la sécurité informationnelle**	
Version n^{o} 1	**Entrée en vigueur** : 2016-11-01	**Révisée le** : S. O.
☒ **Politique organisationnelle** ☐ **Politique de gestion interne** ☐ **Politique spécifique**		
Champ d'application : Directeurs, gestionnaires, médecins, employés et administrateurs		
Installation(s) : ☒ Toutes les installations du CIUSSS MCQ		
Territoire(s) visé(s) : ☒ Tous les territoires du CIUSSS MCQ		
Service(s) visé(s) : ☒Tous les services du CIUSSS MCQ		
Document(s) associé(s) : Cadre de gestion de la sécurité de l'information; PO-10-002 Politique de gestion de la documentation administrative; PO-10-004 Politique d'accès aux documents administratifs et aux renseignements personnels; PO-16-002 Politique d'accès aux renseignements personnels concernant l'usager.		

1. PRÉAMBULE

Le ministère de la Santé et des Services sociaux (MSSS) a adopté, en septembre 2002, le Cadre global de gestion des actifs informationnels – volet sécurité (CGGAI). Celui-ci décrit un ensemble d'énoncés et de principes, les rôles et responsabilités ainsi que les mesures de sécurité que les organismes du Réseau de la santé et des services sociaux (RSSS) doivent respecter et mettre en œuvre.

La mise en œuvre du CGGAI a permis d'introduire une culture de sécurité de l'information dans le RSSS et d'améliorer le niveau global de sécurité. Toutefois, l'évolution des pratiques, la modernisation des services et les nouvelles exigences du Secrétariat du Conseil du trésor (SCT) en matière de sécurité de l'information augmentent les besoins d'échanges d'information et de mobilité des intervenants en santé et services sociaux. Ces nouveaux besoins rendent nécessaire l'évolution de l'encadrement de la sécurité de l'information.

Pour se donner les conditions permettant de relever ces défis et considérant l'apport grandissant des technologies de l'information à l'innovation et à la transformation de la pratique clinique, le ministre de la Santé et des Services sociaux reconnaît la nécessité d'assurer la disponibilité, l'intégrité et la confidentialité de l'information. Pour ce faire, il a mis en place une gouverne claire de la sécurité de l'information.

La présente politique est adoptée en application du paragraphe (a) du premier alinéa de l'article 7 de la Directive sur la sécurité de l'information gouvernementale du Secrétariat du Conseil du trésor (SCT), décret 7-2014, qui confère aux organismes relevant du dirigeant réseau de l'information (DRI) de nouvelles obligations en matière de sécurité de l'information, de protection des renseignements personnels et de respect de la vie privée.

Finalement, la protection des actifs informationnels s'articule autour de deux grands axes, à savoir respectivement :

La sécurité des données :

- **Actif informationnel :** Actif informationnel au sens de la LPCRS , soit une banque d'information, un système d'information, un réseau de télécommunication, une infrastructure technologique ou un ensemble de ces éléments ainsi qu'une composante informatique d'un équipement médical spécialisé ou ultra spécialisé. Est également considéré comme un actif informationnel, tout support papier contenant de l'information.
- **Disponibilité :** Propriété d'une information d'être accessible en temps voulu et de la manière requise par une personne autorisée.
- **Intégrité :** Propriété d'une information de ne subir aucune altération ou destruction de façon erronée ou sans autorisation et d'être conservée sur un support lui procurant stabilité et pérennité. L'intégrité fait référence à l'exactitude et à la complétude.
- **Confidentialité :** Propriété d'une information de n'être accessible, ni divulguée qu'aux personnes ou entités désignées et autorisées.
- **Cycle de vie de l'information :** Ensemble des étapes que franchit une information et qui vont de sa création, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction, en conformité avec le calendrier de conservation de l'organisme.
- **Gestion intégrée des risques de sécurité :** Approche de gestion des risques qui repose sur une gestion globale, proactive et continue des risques de sécurité à tous les niveaux hiérarchiques de l'organisation.
- **Réseau :** Ensemble des organismes qui relèvent du dirigeant réseau de l'information (DRI) de la santé et des services sociaux en vertu de l'article 2, paragraphe 5 de la loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LGGRI).
- **Risque de sécurité de l'information :** Probabilité que survienne un événement préjudiciable, plus ou moins prévisible, qui peut affecter la réalisation des objectifs de l'organisme ou du Réseau.

Sécurité des actes posés pour accéder aux données :

- **Authentification** : acte permettant d'établir la validité de l'identité d'une personne ou d'un dispositif. Par exemple, un mot de passe ou une empreinte digitale constitue des mécanismes d'authentification valables.
- **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. En d'autres termes, c'est la capacité de laisser une trace précise des actes posés à un actif informationnel.

2. BUT DE LA POLITIQUE

Le CIUSSS MCQ met en place la présente politique de sécurité de l'information pour déterminer l'utilisation appropriée et sécuritaire de l'information et des technologies de l'information.

3. OBJECTIFS DE LA POLITIQUE

- Assurer la disponibilité, l'intégrité et la confidentialité à l'égard de l'utilisation des actifs informationnels manipulés par l'organisation;
- Assurer le respect de la vie privée des usagers, notamment la confidentialité des renseignements à caractère nominatif relatifs aux usagers et au personnel du réseau sociosanitaire;
- Assurer la conformité aux lois et règlements applicables ainsi qu'aux directives, normes et orientations gouvernementales;
- Structurer la prise en charge de la sécurité de l'information au sein du CIUSSS MCQ.

4. DÉFINITIONS

Pour la présente politique, les termes et expressions suivantes signifient :

1. **L'organisation :** Centre intégré universitaire de santé et de services sociaux de la Mauricie-et-du-Centre-du-Québec (CIUSSS MCQ);

2. **Actif informationnel :** Actif informationnel au sens de la Loi concernant le partage de certains renseignements de santé (LPCRS), soit une banque d'information, un système d'information, un réseau de télécommunication, une infrastructure technologique ou un ensemble de ces éléments ainsi qu'une composante informatique d'un équipement médical spécialisé ou ultra spécialisé. Est également considéré comme un actif informationnel, tout support papier contenant de l'information;

3. **Confidentialité :** Propriété d'une information de n'être accessible, ni divulguée qu'aux personnes ou entités désignées et autorisées;

4. **Cycle de vie de l'information :** Ensemble des étapes que franchit une information et qui vont de sa création, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction, en conformité avec le calendrier de conservation de l'organisation;

5. **Disponibilité :** Propriété d'une information d'être accessible en temps voulu et de la manière requise par une personne autorisée;

6. **Gestion intégrée des risques de sécurité :** Approche de gestion des risques qui repose sur une gestion globale, proactive et continue des risques de sécurité à tous les niveaux hiérarchiques de l'organisation;

7. **Intégrité :** Propriété d'une information de ne subir aucune altération ou destruction de façon erronée ou sans autorisation et d'être conservée sur un support lui procurant stabilité et pérennité. L'intégrité fait référence à l'exactitude et à la complétude;

8. **Réseau :** Ensemble des organisations qui relèvent du dirigeant réseau de l'information (DRI) de la santé et des services sociaux en vertu de l'article 2, paragraphe 5 de la loi sur la gouvernance et la gestion des ressources informationnelles des organisations publiques et des entreprises du gouvernement (LGGRI);

9. **Risque de sécurité de l'information :** Probabilité que survienne un événement préjudiciable, plus ou moins prévisible, qui peut affecter la réalisation des objectifs de l'organisation ou du Réseau;

10. **Utilisateur:** Toute personne de l'organisme de quelque catégorie d'emploi, de statut d'employé, médecin, administrateur, étudiant ou stagiaire ainsi que toute personne morale ou physique qui, par engagement contractuel ou autrement, utilise un actif informationnel sous la responsabilité de l'organisme où elle a accès.

5. CONTEXTE LÉGAL ET/OU CONTRACTUEL

La présente section répertorie les principales lois, règlements, directives et autres références qui sous-tendent la politique.

QUÉBEC. Loi sur les services de santé et les services sociaux (LRQ, c. S-4.2).
QUÉBEC. Charte des droits et libertés de la personne (LRQ, c C-12).
QUÉBEC. Loi sur l'accès aux documents des organisations publics et sur la protection des renseignements personnels (LRQ, c. A-2.1).

QUÉBEC. Loi sur les archives (LRQ, c. A-21.1).
QUÉBEC. Loi sur la protection de la jeunesse (LRQ, c. P 34.1).
QUÉBEC. Code civil du Québec.
QUÉBEC. Codes de déontologie des différentes professions de la santé.
CANADA. Charte canadienne des droits et libertés de la personne.
CANADA. Loi concernant le droit d'auteur (C-42).
CANADA. Loi sur les jeunes contrevenants.
CANADA. Code criminel.
Commission d'accès à l'information du Québec (CAIQ). 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 (CAIQ). Le courrier électronique.
Commission d'accès à l'information du Québec (CAIQ). Utilisation des télécopieurs.
Conseil du trésor du Québec. Directive concernant la sécurité de l'information électronique et des actifs informationnels. (Loi sur l'administration financière LRQ, c. A-6 article 22).
Conseil du trésor du Québec. Directive sur la sécurité de l'information et des échanges électroniques dans l'Administration gouvernementale.
Conseil du trésor du Québec. Sécurité des échanges électroniques au gouvernement du Québec.
MSSS. RTSS Politique intérimaire de sécurité visant les actifs informationnels du réseau de la santé et des services sociaux.
MSSS. RTSS Exigences minimales en matière de sécurité pour les applications du RTSS.
MSSS. Le cadre global de gestion sur la sécurité des actifs informationnels du réseau de la santé et des services sociaux, version 3.2.

6. MODALITÉS

La politique de sécurité s'applique de façon plus spécifique et non limitative à chacun des points suivants.

Principes de sécurité à respecter lors de l'utilisation des actifs informationnels

Tous les actifs informationnels doivent être dédiés et réservés en priorité à la réalisation des activités de l'organisation.

L'utilisation des actifs informationnels est un *privilège*[1].

Ce privilège peut être révoqué, en tout temps, à tout utilisateur qui ne se conformera pas à la politique.

Tout usage des actifs informationnels qui est dérogatoire à la politique peut être sanctionné selon les dispositions pertinentes de la présente politique, ou toute autre source conventionnelle, légale ou réglementaire à la disposition de l'organisation.

- *Confidentialité des informations et des utilisateurs*

  Conformément à la Loi sur les services de santé et les services sociaux ainsi qu'à la Loi sur l'accès aux documents des organisations publics et la protection des renseignements personnels, tout renseignement nominatif relatif aux usagers contenu dans quelque élément des actifs informationnels de l'organisation est confidentiel.

  L'utilisateur ne doit, autrement que dans le cadre de ses fonctions, consulter, divulguer, modifier ou détruire une information confidentielle.

  L'accès aux informations confidentielles doit être contrôlé par des mesures de sécurité adéquates (ex. : journalisation).

  Toute personne détenant des informations confidentielles dans son milieu de travail, à sa résidence ou dans un autre lieu, doit assurer la sécurité physique des supports (ex. : ordinateur portable, clé USB, téléphone intelligent, tablette numérique) contenant lesdites informations.

  L'utilisateur ne peut pas invoquer son droit à la confidentialité dans les cas où il fait une utilisation contraire à la présente politique.

  Les actifs informationnels sont mis à la disposition des utilisateurs pour l'exécution de leurs tâches. Aucun utilisateur ne peut prétendre à une expectative de vie privée en utilisant les actifs informationnels de l'organisation.

  Toutes les informations relatives aux mesures de sécurité sont confidentielles.

- *Respect des droits d'auteur*[2]

  Personne ne peut effectuer ou participer à la reproduction de logiciels, de progiciels, d'objets numérisés ou de leur documentation, à l'exception du personnel autorisé et pour des fins de copies de sauvegarde et selon les termes des licences d'utilisation qui les régissent.

[1] Autorisation de nature personnelle accordée à un utilisateur des actifs informationnels et régissant son exploitation de ceux-ci, conformément à la politique et ses normes.

[2] Droit exclusif de produire ou de reproduire une œuvre ou une partie importante de celle-ci, sous une forme matérielle quelconque, de la représenter en public, de la publier, de permettre l'un des actes ci-dessus énumérés ainsi que tous les droits accessoires y afférents, le tout tel que prévu par la Loi concernant le droit d'auteur.

Personne ne peut utiliser de reproductions illicites de logiciels, de progiciels ou d'objets numérisés à l'aide des actifs informationnels de l'organisation.

L'utilisation d'un logiciel doit toujours se faire avec égard des droits d'auteurs dudit logiciel.

- *Modifications aux réseaux*

  Il est interdit à tout utilisateur de modifier les *configurations réseau*[3] des actifs informationnels.

  Il est interdit pour un utilisateur d'ajouter un logiciel à quelque actif informationnel.

  Toute modification doit être exécutée selon les procédures et directives prévues à cette fin.

  Les ordinateurs portables contenant des informations appartenant à l'organisation sont aussi visés par cette interdiction.

- *Utilisation de périphériques portables*

  Chaque utilisateur d'ordinateur portable ou de tout autre périphérique portable, contenant ou pouvant contenir des informations confidentielles, doit protéger celui-ci en tout temps contre le vol ou son accès non autorisé par des tiers.

  Toutes les conditions relatives aux sauvegardes de données s'appliquent à tout périphérique portable.

- *Utilisation de la technologie sans fil*

  Aucun équipement (commutateur, aiguilleur) ne pourra être ajouté ou branché au réseau sans le consentement du responsable de la sécurité de l'information (RSI).

  Ces équipements doivent être configurés afin de respecter les normes les plus strictes de codification des données de l'industrie de façon à ne pas permettre le branchement au réseau par une personne de l'extérieur ou l'interception de données sensibles par une tierce partie.

  Seule la direction des ressources informationnelles (DRI) a l'autorité de procéder à l'utilisation du réseau sans fil. Les informations véhiculées sur le réseau sans fil seront journalisées de façon systématique.

Principes de sécurité à respecter lors de la création, manipulation et destruction de données sur les actifs informationnels

- *Propriété des informations*

  Toute information générée par les utilisateurs est la propriété exclusive de l'organisation.

  Toute information qui circule ou réside sur n'importe quel actif informationnel de l'organisation et qui n'a pas été spécifiquement identifiée comme étant la propriété exclusive d'une tierce partie est réputée appartenir à l'organisation.

  L'organisation protège adéquatement toute information qui lui est confiée par une tierce partie ainsi que ses marques de commerce et autres biens couverts par les lois appropriées en matière de propriété intellectuelle.

[3] Toute information requise pour se brancher à un réseau de télécommunications.

- *Sauvegarde des données*

  Toutes les informations qui ont une importance en disponibilité, en confidentialité ou en intégrité doivent faire l'objet de mesures de sauvegarde à une fréquence jugée pertinente, après entente entre le détenteur de l'actif informationnel et la direction des ressources informationnelles.

  Pour rencontrer les objectifs de protection et de disponibilité des informations contenues dans les actifs informationnels, chaque utilisateur est responsable de sauvegarder l'information aux endroits désignés par l'équipe informatique.

- *Encodage des données*

  Toute information confidentielle détenue et transmise par le biais des actifs informationnels doit être préalablement encodée selon les normes, lorsque des mécanismes d'encodage sont disponibles.

- *Destruction des informations*

  Toute information contenue sur les actifs informationnels doit être détruite de façon adéquate selon les normes établies et dans le respect des calendriers de conservation.

Principes de sécurité à respecter lors de l'accès aux actifs informationnels

- *Authentification*

  Lorsque requis, chaque utilisateur doit choisir un ou des mots de passe pour exercer son ou ses privilèges d'accès aux actifs informationnels.

  Il est strictement interdit de partager un mot de passe associé à un nom d'utilisateur. Aucune circonstance ne permet de le justifier à l'exception de celles autorisées spécifiquement par le RSI de l'organisation. Le manquement à cette interdiction rend l'utilisateur fautif responsable de toutes les actions posées par l'individu en possession de ce même mot de passe et certains ou tous ses privilèges d'accès peuvent être révoqués.

- *Privilèges d'accès*

  Tous les privilèges d'accès aux actifs informationnels doivent être octroyés aux utilisateurs en fonction de leurs besoins justifiés. Aucun privilège ne doit être octroyé au-delà des besoins pour l'exécution complète des tâches assignées ou des mandats confiés.

  Compte tenu des caractéristiques de certaines applications, l'octroi de privilèges peut ouvrir l'accès à des informations non nécessaires pour l'exécution des tâches assignées ou des mandats confiés; dans ces cas, l'utilisateur est tenu de s'abstenir d'accéder aux informations non nécessaires pour l'exécution des tâches assignées ou des mandats confiés.

Principes de sécurité à respecter lors de relations avec les tiers[4]

L'organisation doit émettre des normes concernant ses relations avec les tiers en matière de sécurité informationnelle. Des ententes écrites doivent être conclues avec chaque tiers requérant un accès aux actifs informationnels de l'organisation.

Droit de regard

- Le CIUSSS MCQ exerce, en conformité avec la législation et la réglementation en vigueur, un droit de regard sur tout usage des actifs informationnels de l'organisation;
- Des mécanismes sont mis en place pour permettre au CIUSSS MCQ de démontrer au ministre de la Santé et des Services sociaux une prise en charge maîtrisée de la sécurité de l'information à leur niveau organisationnel, conformément à la directive sur la sécurité de l'information gouvernementale.

Sanctions

La présente politique est accompagnée de plusieurs directives.

Lorsqu'un utilisateur déroge à la présente politique ou aux directives en découlant, il s'expose, selon le cas, à des mesures disciplinaires, administratives ou légales en fonction de la gravité de son geste.

7. RÔLES ET RESPONSABILITÉS

Le conseil d'administration du CIUSSS MCQ

Le conseil d'administration du CIUSSS MCQ :

1. adopte la politique et le plan d'action établis par l'organisation en matière de sécurité de l'information, lesquels sont conformes à la politique provinciale de sécurité de l'information et au cadre de gestion de la sécurité de l'information, et suit leur application dans l'établissement;
2. reçoit et entérine annuellement ou au besoin le bilan de sécurité de l'information de l'organisation.

Le président-directeur général, ou en son absence, le président-directeur général adjoint

En tant que premier responsable de la sécurité de l'information de l'organisation, le président directeur général :

1. s'assure du respect des lois et des règles de sécurité de l'information s'appliquant au Réseau, notamment celles émises par le SCT;
2. approuve le cadre de gestion de la sécurité de l'information adapté à l'organisation;
3. s'assure de la mise en œuvre de la politique de sécurité de l'information adoptée par le conseil d'administration et des rôles et responsabilités du cadre de gestion de la sécurité de l'organisation;

[4] Toute personne physique ou morale qui n'est pas directement à l'emploi de l'organisme.

4. nomme un employé de la classe d'emploi cadre à titre de RSI de l'organisation et s'assure de lui octroyer les pouvoirs et ressources nécessaires à la réalisation de ses tâches et responsabilités; le formulaire de nomination du RSI doit être retourné annuellement au 1er avril ou au besoin au responsable organisationnel de la sécurité de l'information (ROSI) lors d'un changement du RSI;
5. établit avec son RSI une relation de forte collaboration lui permettant d'être au fait de toute situation à risque et de tout incident majeur de sécurité de l'information;
6. informe et mobilise ses gestionnaires et l'ensemble de son personnel au sujet de l'application des bonnes pratiques en sécurité de l'information;
7. s'assure de la gestion adéquate des risques de sécurité de l'information en lien avec son contexte organisationnel;
8. s'assure de la nomination des détenteurs de la sécurité de l'information pour l'organisation afin d'assurer la sécurité de l'information et des ressources qui la sous-tendent;
9. s'assure de la mise en place d'un comité chargé de la sécurité de l'information au sein de l'organisation et mandate le RSI pour présider ce comité.

Le responsable de la sécurité de l'information (RSI)

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

1. planifie les activités nécessaires à la mise en place de la sécurité de l'information au sein de l'organisation;
2. s'assure de l'encadrement de la sécurité de l'information au sein de l'organisation, veille à l'application de la politique et du cadre de gestion de la sécurité de l'information de l'organisation et s'assure du respect par l'organisation des règles particulières publiées par le DRI en matière de sécurité de l'information;
3. agit à titre de porte-parole du ROSI auprès de l'organisation en informant les différents intervenants en sécurité de l'information des orientations et des priorités d'intervention provinciale et s'assure de leur mise en œuvre;
4. représente l'organisation au Comité provincial de la sécurité de l'information du réseau et s'assure de la participation de l'organisation aux processus provinciaux de gestion de la sécurité de l'information;
5. dirige la coordination et la cohérence des activités de sécurité de l'information menées au sein de l'organisation, notamment ceux de l'officier de sécurité de l'information et du conseiller en gouvernance de la sécurité, le cas échéant;
6. préside pour le compte du dirigeant de l'organisation, le comité de sécurité de l'information au sein de l'organisation et lui soumet pour consultation, les orientations, les politiques, les directives, les cadres de gestion, les plans d'action, les bilans et les rapports sur les événements ayant mis ou qui auraient pu mettre en péril la sécurité de l'information de l'organisation, ainsi que toute proposition d'action ou état d'avancement des projets destinés au dirigeant de l'organisation;

7. s'assure de la mise en place du registre d'autorité de la sécurité de l'information, dans lequel sont notamment consignés les noms des détenteurs de l'information et les systèmes d'information qui leur sont assignés;
8. s'assure de la mise en œuvre d'un système de gestion intégré des risques de sécurité de l'information, qui lui permet de maîtriser les risques de sécurité relatifs à l'organisation;
9. s'assure de la mise en œuvre d'un processus de gestion des incidents de sécurité de l'information dans l'organisation;
10. veille à l'identification et à la prise en charge des exigences de sécurité de l'information lors de la réalisation de projets de développement ou de l'acquisition de systèmes d'information;
11. s'assure de l'intégration aux ententes de services et aux contrats, des dispositions garantissant le respect des exigences de sécurité de l'information en prenant appui sur le cadre gouvernemental d'élaboration de clauses contractuelles en matière de sécurité de l'information et de protection des renseignements personnels;
12. veille à la mise en œuvre de toute recommandation jugée pertinente découlant d'une vérification ou d'un audit de sécurité;
13. s'assure de l'élaboration et de la mise en œuvre d'un programme formel de formation et de sensibilisation en matière de sécurité de l'information;
14. s'assure de la production d'un bilan annuel ou, au besoin, d'un plan d'action triennal de la sécurité de l'information de l'organisation, les valide et les transmet au ROSI du Réseau et à son dirigeant d'organisation;
15. rend compte des réalisations de l'organisation en matière de sécurité de l'information au ROSI du Réseau et à son dirigeant d'organisation;
16. évalue constamment toute information reçue en lien avec la sécurité de l'information.

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

Le conseiller en gouvernance de la sécurité

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

1. accompagne le RSI dans la définition des orientations stratégiques, des directives et des plans d'action en matière de sécurité de l'information;
2. participe à la rédaction des documents d'encadrement de la sécurité de l'information de l'organisation, notamment la politique et le cadre de gestion de sécurité de l'information;
3. accompagne le RSI dans la mise en œuvre des orientations internes découlant des directives ministérielles et celles du DRI, des politiques internes et des pratiques généralement admises à cet égard;

4. participe à la définition et accompagne le RSI dans la mise en œuvre de processus formels de gestion de la sécurité de l'information;
5. accompagne les directions partenaires en matière de sécurité de l'information et participe à l'intégration de dispositions garantissant le respect des exigences de sécurité de l'information dans les ententes de services et les contrats;
6. assiste les détenteurs de l'information dans la catégorisation de l'information relevant de leur responsabilité, dans l'identification et l'évaluation des situations de risques ainsi que dans la définition de plans d'action visant à réduire les risques de sécurité de l'information à un niveau acceptable pour l'organisation et pour le MSSS;
7. identifie et prend en charge les exigences de sécurité de l'information lors de la réalisation de projets de développement ou de l'acquisition de systèmes d'information;
8. élabore et met en œuvre le programme de formation et de sensibilisation en matière de sécurité de l'information;
9. tient à jour le registre d'autorité de la sécurité de l'information;
10. assure la coordination et la réalisation de projets de sécurité de l'information;
11. produit les bilans et les plans d'action de sécurité de l'information de l'organisation.

L'officier de sécurité de l'information

L'officier de sécurité de l'information est un professionnel de la sécurité de l'information ayant les compétences nécessaires à la réalisation des tâches et responsabilités suivantes. Il :

1. contribue à la mise en place des activités opérationnelles de sécurité de l'information, plus précisément la planification, le déploiement, l'exécution, la surveillance, les enquêtes et l'amélioration des processus de sécurité nécessaires à la gestion opérationnelle de la sécurité dans l'organisation, la gestion des risques et la gestion des incidents en respectant les exigences de sécurité définies dans les règles particulières et conformément aux pratiques recommandées de l'industrie;
2. participe activement au réseau d'alerte du Réseau pour la gestion des incidents de sécurité de l'information;
3. contribue aux analyses de risques de sécurité de l'information, identifie les menaces et les situations de vulnérabilité et met en œuvre les solutions appropriées;
4. supporte le RSI et le conseiller en gouvernance de la sécurité dans les activités de développement et d'acquisition, pour le volet technique de la sécurité dans le respect des exigences de sécurité définies dans les règles particulières et conformément aux pratiques recommandées;
5. participe aux comités de gestion des changements, s'il y a lieu, et possède un droit de réserve face à des changements qu'il juge trop risqués sur le plan de la sécurité de l'information;
6. s'assure de la production des rapports des processus de sécurité de l'information (incidents, vulnérabilités, etc.) et les transmet à son RSI, avec son appréciation et des justifications, au besoin.

Le Comité de sécurité de l'information de l'organisation

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

1. examine et formule des recommandations concernant les orientations, les politiques, les directives, les cadres de gestion, les plans d'action et les bilans de l'organisation, ainsi que toute proposition d'action ou état d'avancement de projets en sécurité de l'information;
2. s'assure de la prise en charge des risques, des situations vulnérables ou des incidents identifiés;
3. analyse et formule des recommandations concernant les événements ayant mis ou qui auraient pu mettre en péril la sécurité de l'information de l'organisation.

Ce comité est présidé par le RSI, à titre de représentant du dirigeant de l'organisation. Il est constitué des détenteurs de l'information ainsi que des unités administratives responsables des ressources informationnelles, de la vérification interne, de l'accès à l'information et de la protection des renseignements personnels, de la gestion documentaire, de la sécurité physique et de l'éthique, ainsi que sur invitation, toute personne jugée pertinente.

Les responsables de domaines connexes à la sécurité de l'information

Les responsables de domaines connexes à la sécurité veillent au respect des exigences de sécurité relatives à leur domaine. À ce titre, ils :

1. communiquent au RSI de l'organisation les problématiques et les préoccupations de sécurité en rapport avec leur domaine;
2. contribuent à assurer la cohérence et l'harmonisation des interventions en sécurité de l'information, y compris lors de la mise en œuvre du processus de gestion des risques et des incidents de sécurité de l'information;
3. participent au comité de sécurité de l'information de l'organisation.

Selon les organisations, il peut s'agir notamment, sans s'y limiter, du :

1. responsable de la gestion des technologies de l'information;
2. responsable de l'architecture d'entreprise, volet sécurité;
3. responsable de l'accès à l'information et de la protection des renseignements personnels;
4. responsable de la vérification interne;
5. responsable de la sécurité physique;
6. responsable de la gestion documentaire;
7. responsable de la continuité des services;
8. responsable de l'éthique;
9. responsable de la gestion de la qualité et des risques organisationnels.

Les détenteurs de l'information

Les détenteurs de l'information sont responsables d'assurer la sécurité d'un ou de plusieurs actifs informationnels qui leur sont confiés par le sous-ministre ou le dirigeant de l'organisation. Notamment, ils :

1. s'impliquent dans l'ensemble des activités relatives à la sécurité, notamment la catégorisation, l'évaluation des risques, la détermination du niveau de protection visé, l'élaboration des contrôles non technologiques et, finalement, la prise en charge des risques résiduels;
2. s'assurent de connaître et évaluer les risques et vulnérabilités de leurs actifs informationnels, priorisent les actions correctives appropriées et gèrent leur application selon le plan d'action déterminé;
3. s'assurent que les mesures de sécurité appropriées sont élaborées, approuvées, mises en place et appliquées systématiquement;
4. s'assurent que leur nom et les actifs informationnels dont ils assument la responsabilité sont consignés dans le registre d'autorité;
5. déterminent les règles d'accès aux actifs informationnels dont ils assument la responsabilité avec l'appui du RSI de l'organisation.

Les gestionnaires

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

1. informent leur personnel des dispositions de la politique de sécurité de l'information et de toute directive, standard et procédure en vigueur en matière de sécurité de l'information ainsi que des modalités liées à leur mise en œuvre, et les sensibilisent à la nécessité de s'y conformer;
2. s'assurent que les actifs informationnels mis à la disposition de son personnel sont utilisés en conformité avec les principes généraux et les exigences de la politique de sécurité de l'information et des règles particulières;
3. s'assurent que la sécurité de l'information est prise en compte dans tout contrat ou entente de services attribué par leur unité administrative et voient à ce que tout consultant, partenaire (ex. : stagiaire) ou fournisseur s'engage à respecter et respecte les règles de sécurité de l'information de l'organisation.

Les utilisateurs

Les utilisateurs dûment autorisés à accéder aux actifs informationnels du Réseau :

1. appliquent et respectent les lois et règlements qui régissent leur domaine d'activités ainsi que toutes les politiques, directives, mesures, processus et procédures en matière de sécurité de l'information auxquels ils sont assujettis soit par leur lien d'emploi, par contrat ou par entente;
2. avisent leur supérieur immédiat de toute situation portée à leur connaissance et qui est susceptible de compromettre la sécurité de l'information.

8. SIGNATURES

<table>
<tr><td>ÉLABORATION :</td><td colspan="2">Daniel Brouillette
Directeur
Direction des ressources informationnelles</td></tr>
<tr><td>COLLABORATION :</td><td colspan="2">Bernard Gauthier
Chef de service – Infrastructure technologique</td></tr>
<tr><td rowspan="12">ANNULE ET REMPLACE :</td><td>CJMCQ</td><td>Politique relative à la sécurité des actifs Informationnels, 2011</td></tr>
<tr><td>CRDITED</td><td>Politique relative à la sécurité des actifs Informationnels, DRFMI-506-2013-01</td></tr>
<tr><td>Domrémy</td><td>Politique relative à la sécurité des actifs Informationnels, RT-803</td></tr>
<tr><td>InterVal</td><td>Politique relative à la sécurité des actifs Informationnels, DSA-POL-2013</td></tr>
<tr><td>CSSSAE</td><td>Politique relative à la sécurité des actifs Informationnels, DRIP-005, 2014</td></tr>
<tr><td>CSSSBNY</td><td>Politique relative à la sécurité des actifs Informationnels, PO-CA-2014-07</td></tr>
<tr><td>CSSSD</td><td>Politique relative à la sécurité des actifs Informationnels, PC-15 2010</td></tr>
<tr><td>CSSSVB</td><td>Politique relative à la sécurité des actifs Informationnels, POL-5000-03 2014</td></tr>
<tr><td>CSSSHSM</td><td>Politique relative à la sécurité des actifs Informationnels, DSA&T-14</td></tr>
<tr><td>CSSSÉ</td><td>Politique relative à la sécurité des actifs Informationnels, PO-05 2014</td></tr>
<tr><td>CSSSTR</td><td>Politique relative à la sécurité des actifs Informationnels, PO-104 2006</td></tr>
<tr><td>ADOPTÉE PAR :</td><td colspan="2">Le conseil d’administration du CIUSSS MCQ

Original signé par
_____
Marc Descôteaux, vice-président</td></tr>
<tr><td>RÉVISION :</td><td colspan="2">2019</td></tr>
</table>

Annexe A – Aide-mémoire pour les utilisateurs d'actifs informationnels

Ce petit aide-mémoire se veut être un rappel des points les plus importants de la politique. Il ne remplace pas une lecture complète et régulière de la politique de sécurité des actifs informationnels.

L'axe important autour duquel s'articule la protection des actifs informationnels :

La sécurité des données

- Disponibilité : propriété d'une information d'être accessible et utilisable en temps voulu et de la manière requise par une personne autorisée.
- Intégrité : propriété d'une information ou d'une technologie de l'information de n'être ni modifiée, ni altérée, ni détruite sans autorisation.
- Confidentialité : propriété d'une information accessible uniquement aux personnes autorisées.

Utilisation des actifs informationnels

L'utilisation des actifs informationnels est un privilège. Ce privilège peut être révoqué en tout temps, à tout utilisateur qui ne se conformera pas à la politique.

Droit d'auteur

L'utilisation d'un logiciel doit toujours se faire avec égard des droits d'auteur dudit logiciel.

Authentification

Il est strictement interdit de partager un mot de passe. Aucune circonstance ne permet de le justifier à l'exception de celle autorisée spécifiquement par le responsable de la sécurité de l'information de l'organisation. Le manquement à cette interdiction rend l'utilisateur fautif responsable de toutes les actions posées par l'individu en possession de ce même mot de passe et certains ou tous ses privilèges d'accès peuvent être révoqués.

Vie privée

Les actifs informationnels sont mis à la disposition des utilisateurs pour l'exécution de leurs tâches. Aucun utilisateur ne peut prétendre à une expectative de vie privée en utilisant ses actifs informationnels de l'organisation.

Rôles et responsabilités des utilisateurs d'actifs informationnels

Chaque utilisateur est responsable de respecter la présente politique, les normes, les directives et les procédures en vigueur en matière de sécurité de l'information et d'informer son responsable de toute violation des mesures de sécurité dont il pourrait être témoin ou de toute anomalie décelée pouvant nuire à la protection des actifs informationnels.