Centre intégré universitaire de santé et de services sociaux de l'Est-de-l'Île-de-Montréal
Québec

Direction générale adjointe

POLITIQUE

GESTION DES INCIDENTS DE SÉCURITÉ DE L'INFORMATION		
Nº Politique : **POL 061**	Responsable de l'application : Le responsable de la sécurité de l'information (RSI)	
Nº Procédure découlant : **s.o.**		
Approuvée par : **Comité de direction**	Date d'approbation : **2019-02-26**	Date de révision : **2023-02-26**
Destinataires : Toutes les parties prenantes internes et externes du processus de gestion des incidents de sécurité de l'information (DRT, DQÉPÉ, DST, toutes les directions détentrices de l'information et l'équipe de sécurité de l'information, les fournisseurs et autres partenaires), ainsi que tous les utilisateurs des actifs informationnels du CIUSSS-EMTL.		

1 CONTEXTE

La Politique sur la sécurité de l'information gouvernementale, adoptée par le Conseil des ministres en janvier 2014, énonce les obligations des organismes publics en matière de sécurité de l'information. À ce titre, les organismes du réseau de la santé et des services sociaux (RSSS) doivent mettre en place, entre autres, un processus de gestion des incidents de sécurité de l'information[1].

Le Secrétariat du Conseil du trésor (SCT) a de plus publié un Cadre de gestion des risques et incidents à portée gouvernementale, adopté par le Conseil du trésor en décembre 2013. Ce Cadre précise notamment le processus de gestion des incidents à portée gouvernementale que les organismes publics sont dans l'obligation de déclarer.

En vertu de ce cadre normatif global, la présente politique décrit les éléments de gestion que le CIUSSS de l'Est-de-l'Île-de-Montréal (CIUSSS-EMTL) met en place afin de répondre aux exigences du ministère de la Santé et des Services sociaux (MSSS) et du SCT. Ce cadre de gestion des incidents de sécurité de l'information implique tous les partenaires internes, les directions détentrices d'actifs informationnels, ainsi que l'équipe interne de sécurité de l'information.

2 CHAMP D'APPLICATION

L'information visée par la présente politique est celle que le CIUSSS-EMTL détient, dans l'exercice de sa mission, que sa conservation soit assurée par lui-même ou par un tiers, quels que soient son support ou son moyen de communication et ce, tout au long de son cycle de vie.

[1] Directive sur la sécurité de l'information gouvernementale, Article 7, paragraphe C

3 OBJECTIFS

Dans le cadre de l'application des exigences du MSSS, la présente politique vise à décrire et mettre en place le cadre de gouvernance ainsi que le processus de gestion des incidents de sécurité de l'information au CIUSSS-EMTL, afin d'assurer ou de soutenir :

- une prise en charge rapide et adéquate advenant un incident;
- une compréhension commune des rôles et responsabilités des intervenants;
- une gestion optimale des ressources;
- de meilleures communications entre l'ensemble des intervenants.

4 DÉFINITIONS

4.1 Actif informationnel

Un actif informationnel est 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 ultraspécialisé[2].

Un actif informationnel inclut tout document constitué d'information portée par un support papier ou tout type de support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcriptibles sous l'une de ces formes ou en un autre système de symboles[3].

4.2 Continuité des services

Capacité d'une organisation d'assurer, en cas de sinistre, la poursuite de ses processus d'affaires selon un niveau de service prédéfini.

4.3 Déclaration ou requête (de sécurité de l'information)

Action de porter à la connaissance du CIUSSS-EMTL, en suivant la procédure officielle requise selon le type d'événement, tout incident ou risque d'incident de sécurité de l'information constaté par un utilisateur des actifs informationnels du CIUSSS-EMTL ou un témoin de la situation ou de l'événement.

4.4 Dimensions de la sécurité de l'information

- **Disponibilité**

  La disponibilité est la propriété d'une information d'être accessible et utilisable en temps voulu et de manière adéquate par une personne autorisée.

[2] *Loi concernant le partage de certains renseignements de santé*, RLRQ c P-9.0-001, art 3 (1◦)
[3] *Loi concernant le cadre juridique des technologies de l'information*, RLRQ c C-1., art 3.

- **Intégrité**

  L'intégrité est la 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**

  La confidentialité est la propriété d'une information d'être accessible aux seules personnes autorisées.

4.5 Évènement de sécurité de l'information

De manière générale, « évènement » est un terme générique utilisé pour désigner toute situation non souhaitée, redoutée ou indésirable qui a ou aurait pu causer des conséquences sur la confidentialité, l'intégrité ou la disponibilité des informations détenues par le CIUSSS-EMTL. Un événement désigne donc aussi un incident de sécurité de l'information, de nature technologique ou non.

Dans le cas spécifique des technologies de l'information et des communications, un évènement est une occurrence identifiée de l'état d'un service, d'un système ou d'un réseau, indiquant une faille possible dans la politique de sécurité de l'information ou un échec des mesures de sécurité ou encore une situation inconnue jusqu'alors et pouvant relever de la sécurité.

4.6 Incident de sécurité de l'information

Un ou plusieurs évènements liés à la sécurité de l'information indésirables ou inattendus présentant une probabilité forte de compromettre les activités de l'organisation et de menacer la sécurité de l'information (disponibilité, intégrité, confidentialité). Un incident de sécurité de l'information peut être lié ou non à l'utilisation des technologies de l'information et des communications.

Un incident de sécurité de l'information est catégorisé selon son niveau d'impact, de gravité ou de fréquence.

4.7 Incident ou accident lors de la prestation des soins et services de santé[4]

- **Incident**

  Action ou situation qui n'entraîne pas de conséquence sur l'état de santé ou le bien- être d'un usager, du personnel, d'un professionnel concerné ou d'un tiers, mais dont le résultat est inhabituel et qui, en d'autres occasions, pourrait entraîner des conséquences

[4] Politique de Déclaration des incidents et des accidents liés à la sécurité des usagers (POL-032), rubrique Définitions, paragraphes 4.1 et 4.2.; Loi sur les services de santé et les services sociaux, RLRQ c S-4.2 (LSSSS), art. 183.2 et art. 8.

- **Accident**

  Action ou situation où le risque se réalise et est, ou pourrait être, à l'origine de conséquences sur l'état de santé ou le bien-être de l'usager, du personnel, d'un professionnel concerné ou d'un tiers (art.8 de la LSSSS).

4.8 Mesure de sécurité de l'information

Moyen concret assurant, partiellement ou totalement, la protection d'un actif informationnel contre un ou plusieurs risques et dont la mise en œuvre vise à amoindrir la probabilité de survenance de ces risques ou à réduire les pertes qui en résultent[5].

4.9 Plan de continuité des activités

Plan mis en œuvre à l'échelle de l'organisation visant à assurer la continuité globale des opérations après la déclaration d'un incident. Il couvre tous les processus opérationnels de l'organisation dont ceux des ressources informationnelles. Il s'agit, par exemple, des mécanismes de continuité de service mis en place dans les secteurs d'activités pour répondre à un désastre ou à une interruption des systèmes informatiques.

4.10 Plan de relève informatique

Plan de secours permettant de garantir la reprise des activités informatiques après un désastre. Ce plan est essentiellement technique et est mis en place par les ressources informationnelles.

4.11 Ressources informationnelles

Les actifs informationnels ainsi que les ressources humaines, matérielles et financières directement affectées à la gestion, à l'acquisition, au développement, à l'entretien, à l'exploitation, à l'accès, à l'utilisation, à la protection, à la conservation et à l'aliénation de ces actifs.

4.12 Risque de sécurité de l'information

Probabilité que survienne un événement préjudiciable, en termes de disponibilité, d'intégrité et de confidentialité, plus ou moins prévisible, qui peut affecter la réalisation des objectifs de l'organisme. Il est le résultat de la combinaison de la probabilité d'un événement et de ses conséquences.

Le risque est défini à l'aide de ce que l'on nomme « l'équation du risque » :

RISQUE = MENACE × VULNÉRABILITÉ × IMPACT[6]

[5] Office québécois de la langue française – Grand dictionnaire terminologique

[6] Guide de gestion des risques de sécurité de l'information, définitions, Risque de sécurité de l'information, p.5

4.13 Sinistre

Situation provoquée par un évènement dû à un phénomène naturel, une défaillance technologique ou un accident découlant ou non de l'intervention humaine (accidentel ou intentionnel), qui cause des préjudices aux personnes ou des dommages aux biens et exige des mesures inhabituelles[7].

4.14 Système de détection d'intrusion

Système combinant logiciel et matériel, qui permet de détecter en temps réel les tentatives d'intrusion sur un réseau interne ou sur un seul ordinateur hôte, de neutraliser ces attaques réseaux ou systèmes et d'assurer ainsi la sécurité du réseau de l'organisation.

4.15 Usager

Toute personne qui a reçu, aurait dû recevoir, reçoit ou requiert des soins de santé et/ou des services sociaux du CIUSSS-EMTL; ce terme comprend, le cas échéant, tout représentant de l'usager au sens de l'article 12 de la Loi sur les services de santé et les services sociaux, RLRQ c S-4.2 (LSSSS), ainsi que tout héritier ou représentant légal au sens du 1er alinéa de l'article 23 de la LSSSS d'un usager décédé[8].

4.16 Utilisateur

Toute personne oeuvrant ou exerçant sa profession au sein du CIUSSS-EMTL, de quelque catégorie d'emploi et de statut que ce soit, les médecins, les médecins résidents, les dentistes, les pharmaciens, les chercheurs, le personnel de soins et services, administratif ou de soutien, les pairs aidants, les stagiaires, les bénévoles, ainsi que toute personne physique ou morale qui, par engagement contractuel ou autrement, utilise un actif informationnel du CIUSSS-EMTL ou y a accès.

4.17 Vulnérabilité

La vulnérabilité englobe toutes les faiblesses dans les processus et moyens de l'organisation, ainsi que dans son environnement, causant une incapacité partielle à faire face aux événements accidentels, intentionnels (comportements inappropriés des individus), ainsi qu'aux menaces naturelles qui la guettent.

La vulnérabilité spécifique aux technologies de l'information et des communications correspond à la faiblesse d'un système se traduisant par une incapacité partielle de celui-ci à faire face aux menaces informatiques qui le guettent.

---

[7] Adapté du Plan intégré de mesures d'urgence et de sécurité civile (PIMUSC), définition de Sinistre majeur p. 41

[8] Politique de Déclaration des incidents et des accidents liés à la sécurité des usagers (POL-032), rubrique Définitions, paragraphes 4.10

5 ÉNONCÉS ET PRINCIPES DIRECTEURS

Ce document précise les énoncés et les principes directeurs de la mise en œuvre du processus de gestion des incidents :

5.1 NIVEAUX DE SÉVÉRITÉ DES INCIDENTS DE SÉCURITÉ DE L'INFORMATION

Le niveau de sévérité d'un incident de sécurité de l'information[9], est défini selon son impact sur l'organisation. Le dirigeant réseau de l'information (DRI) du MSSS a défini quatre niveaux de sévérité, soit :

- Mineur
- Modéré
- Important
- Critique

Les évaluations selon les grilles des partenaires internes et externes de la gestion des incidents de sécurité de l'information (notamment la DST, la DRT, la DQÉPÉ, les autres directions, les fournisseurs) seront arrimées avec la grille ci-dessous lors des analyses des incidents de sécurité de l'information.

Niveau de sévérité	Description	Exemples
Critique **(à portée gouverne-mentale)**	• Un ou plusieurs services indispensables à la population ne peuvent être rendus. • Met en danger la santé, la vie ou le bien-être de personnes. • Affecte le respect des droits fondamentaux des personnes à la protection de leurs renseignements personnels et de leur vie privée et, de ce fait, met en danger la santé, la vie ou le bien-être de ces personnes. • Affecte la réputation du gouvernement, avec ou sans médiatisation.	Le système d'information clinique (DCI OACIS) est devenu indisponible.

[9] Tel qu'énoncé dans la « Directive MSSS-DIR01 Déclaration des incidents de sécurité »

Niveau de sévérité	Description	Exemples
Important	• Affecte de manière significative la qualité de services indispensables à la population. • Possède un potentiel fort de nuire à la réputation de l'établissement. • Affecte les activités propres à un ou plusieurs autres organismes. • Affecte le respect des droits fondamentaux des personnes à la protection de leurs renseignements personnels et de leur vie privée, sans porter atteinte à la santé, à la vie ou au bien-être de ces personnes.	Des dossiers d'usagers ne sont plus disponibles dans le système clinique centralisé DCI.
Modéré	• Affecte plusieurs secteurs de l'établissement.	Le système de gestion RH n'est plus disponible.
Mineur	• Affecte un secteur d'activité de l'établissement.	Le système de gestion des stationnements a un problème.

5.2 CLASSIFICATION DES INCIDENTS DE SÉCURITÉ DE L'INFORMATION

La classification des incidents de sécurité de l'information vise à établir un langage commun permettant de faciliter leur gestion ainsi que la coordination des actions s'y rapportant. Cette classification est établie en fonction de la nature, du type et du niveau de sévérité de l'incident de sécurité de l'information. Ainsi, le DRI du MSSS considère six classes de classification d'un incident de sécurité de l'information. Toutefois, un incident peut, selon sa nature, appartenir à plus d'une classe.

TABLEAU DE CLASSIFICATION DES INCIDENTS DE SÉCURITÉ DE L'INFORMATION		
1. Tout incident de sécurité de l'information, technologique ou non, caractérisé par un accès non autorisé à un périmètre physique contrôlé (ex. : centres de traitement, local d'archives) et résultant en des accès non autorisés à de l'information ou à une perturbation de la disponibilité des infrastructures technologiques.		
Classe d'incident	**Caractéristiques de l'événement**	***Exemples***

TABLEAU DE CLASSIFICATION DES INCIDENTS DE SÉCURITÉ DE L'INFORMATION		
1.1. **Atteinte à la sécurité physique**	Accès physique aux locaux hébergeant des infrastructures technologiques à la suite de la neutralisation ou du contournement des mécanismes de contrôle d'accès et de surveillance en place.	*Entrée par effraction dans la salle des serveurs informatiques.*
	Accès physique aux locaux hébergeant des documents confidentiels, à la suite de la neutralisation ou du contournement des mécanismes de contrôle d'accès et de surveillance en place.	*Accès non autorisé aux dossiers d'usagers dans une salle sécurisée contenant des archives, en utilisant la carte d'accès d'un utilisateur parti à la retraite.*
2. Tout incident technologique de sécurité de l'information caractérisé par l'installation ou l'exécution réussie (infection) d'un code malicieux sur un système, une application ou un environnement. Les codes malicieux mis avec succès en quarantaine, notamment par un antivirus, ne doivent pas être rapportés.		
Classe d'incident	**Caractéristiques de l'événement**	***Exemples***
2.1 Code malicieux	Présence de code malicieux au sein des infrastructures technologiques du réseau ou de tout dispositif qui s'y relie.	*Détection d'un virus, ver, cheval de Troie, etc.;* *Détection de communications non conformes au fonctionnement normal ou aux politiques de sécurité.*
3. Tout incident de sécurité de l'information, technologique ou non, suite à une négligence, une erreur, une omission ou le non-respect des règles de sécurité.		
Classe d'incident	**Caractéristiques de l'événement**	***Exemples***
3.1 Compor-tement inappro-prié	Utilisation inappropriée de ses privilèges pour accéder à de l'information dans le but d'en tirer un profit, de perturber les services ou de nuire à la réputation de l'organisme ou d'une personne.	*Intervenant du CIUSSS-EMTL accédant à un dossier patient sans que ses tâches le justifient;* *Intervenant technologique accédant aux données hébergées par les composantes sous sa responsabilité.*
	Divulgation intentionnelle d'information sensible ou confidentielle.	*Transmission d'un dossier d'employé à une personne non autorisée.* *Divulgation du mot de passe à un tiers.*
	Transmission, conservation ou élimination non sécuritaire d'information sensible ou confidentielle (exposition élevée à des risques).	*Document sensible dans un bac de récupération non sécurisé;* *Déchiquetage de document sensible (sans règle spécifique);* *Réparation ou mise au rebut d'un dispositif (ex : ordinateur) contenant de l'information sensible.*

TABLEAU DE CLASSIFICATION DES INCIDENTS DE SÉCURITÉ DE L'INFORMATION		
	Non-respect des politiques, règles et code de conduite relatifs à l'acquisition ou l'utilisation des technologies de l'information.	*Divulgation du mot de passe à un tiers;* *Utilisation de solutions technologiques ou procédures ne respectant pas les exigences de sécurité;* *Désactivation des contrôles de sécurité d'un équipement géré par le réseau (modification de la configuration);* *Élaboration de contrat ou d'entente n'intégrant pas des clauses de sécurité de l'information.*
		*Conservation de données sensibles sur un dispositif mobile non autorisé (ex. : portable, téléphone intelligent, etc.); ** *Utilisation d'un service de courriel public (ex. : Gmail) pour transmettre des documents sensibles. *[10]*
4. Tout incident de sécurité de l'information technologique caractérisé par un accès non autorisé et mal intentionné visant principalement à compromettre la confidentialité, l'intégrité ou la disponibilité de l'information ou des infrastructures technologiques.		
Classe d'incident	**Caractéristiques de l'événement**	***Exemples***
4.1 Cyber-attaque	Accès logique illicite aux infrastructures technologiques ou à l'information dû à l'absence, à l'inefficacité ou au contournement des mécanismes de sécurité.	*Attaque sur la base de données;* *Détection d'un code malicieux;* *Attaque technologique;* *Écoute électronique;* *Usurpation d'identité d'un utilisateur;* *Détection de communications non conformes au fonctionnement normal ou aux politiques de sécurité.*

[10] **** À moins que la situation ne l'exige, à cause de la non disponibilité d'un moyen autorisé de sauvegarde ou de transmission de l'information; prendre les précautions nécessaires (encryption, etc.);***
S'assurer de réintégrer l'information requise au dossier officiel et d'effacer les données sur le dispositif ou outil non sécurisé.

TABLEAU DE CLASSIFICATION DES INCIDENTS DE SÉCURITÉ DE L'INFORMATION		
	Événement visant à rendre inopérant les services technologiques ou les télécommunications.	*Attaque par déni de service.*
5. Tout incident de sécurité de l'information technologique ayant pour cause des configurations déficientes de sécurité ou des pannes de l'infrastructure technologique ou d'application, ayant des impacts sur la sécurité de l'information.		
Classe d'incident	**Caractéristiques de l'événement**	***Exemples***
5. 1 Dysfonc-tionne-ment technolo-gique	Accès, modification ou destruction illicite d'information dû à l'absence ou à l'inefficacité des mécanismes de sécurité.	*Mauvaise configuration d'une composante technologique donnant un accès inapproprié à des actifs informationnels;* *Mécanisme de sécurité inopérant à la suite d'une erreur d'opération ou d'un problème technique;* *Absence de sécurité dans la conservation, la communication ou la destruction d'information confidentielle.*
	Accès à des services ou des données non conformes aux politiques de sécurité en place.	*Utilisateur pouvant accéder à un site Web pouvant présenter des risques;* *Accès non contrôlés à des infrastructures technologiques ou à des données.*
	Perturbation des services de soin ou des services technologiques due à l'absence ou à l'inefficacité des mécanismes de sécurité.	*Dysfonctionnement de composantes de sécurité perturbant les communications internes ou externes.*
6. Tout incident de sécurité de l'information, technologique ou non, caractérisé par la perte ou le vol d'information sur support papier ou électronique (ex. : clé USB, ordinateur portatif, etc.).		
Classe d'incident	**Caractéristiques de l'événement**	***Exemples***
6.1 Vol ou perte d'infor-mation	Perte ou vol d'information sensible ou confidentielle, quel que soit le support sur lequel elle se trouve.	*Perte ou vol d'un dispositif contenant des informations sensibles (ex. : ordinateur, cellulaire, clé USB, CD, etc.);* *Perte ou vol de document papier.*

5.3 LE PROCESSUS DE GESTION DES INCIDENTS DE SÉCURITÉ DE L'INFORMATION

Le processus de gestion des incidents de sécurité de l'information du CIUSSS-EMTL s'insère dans un cadre de gestion plus global des événements indésirables, sinistres ou aléas, et d'amélioration continue. Le processus de gestion des incidents de sécurité de l'information met en place une structure d'accueil et de coordination de tels événements indésirables et, afin d'assurer leur pleine prise en charge, se rattache aux politiques, plans, procédures, activités, etc. mis en place par les partenaires internes ou externes.

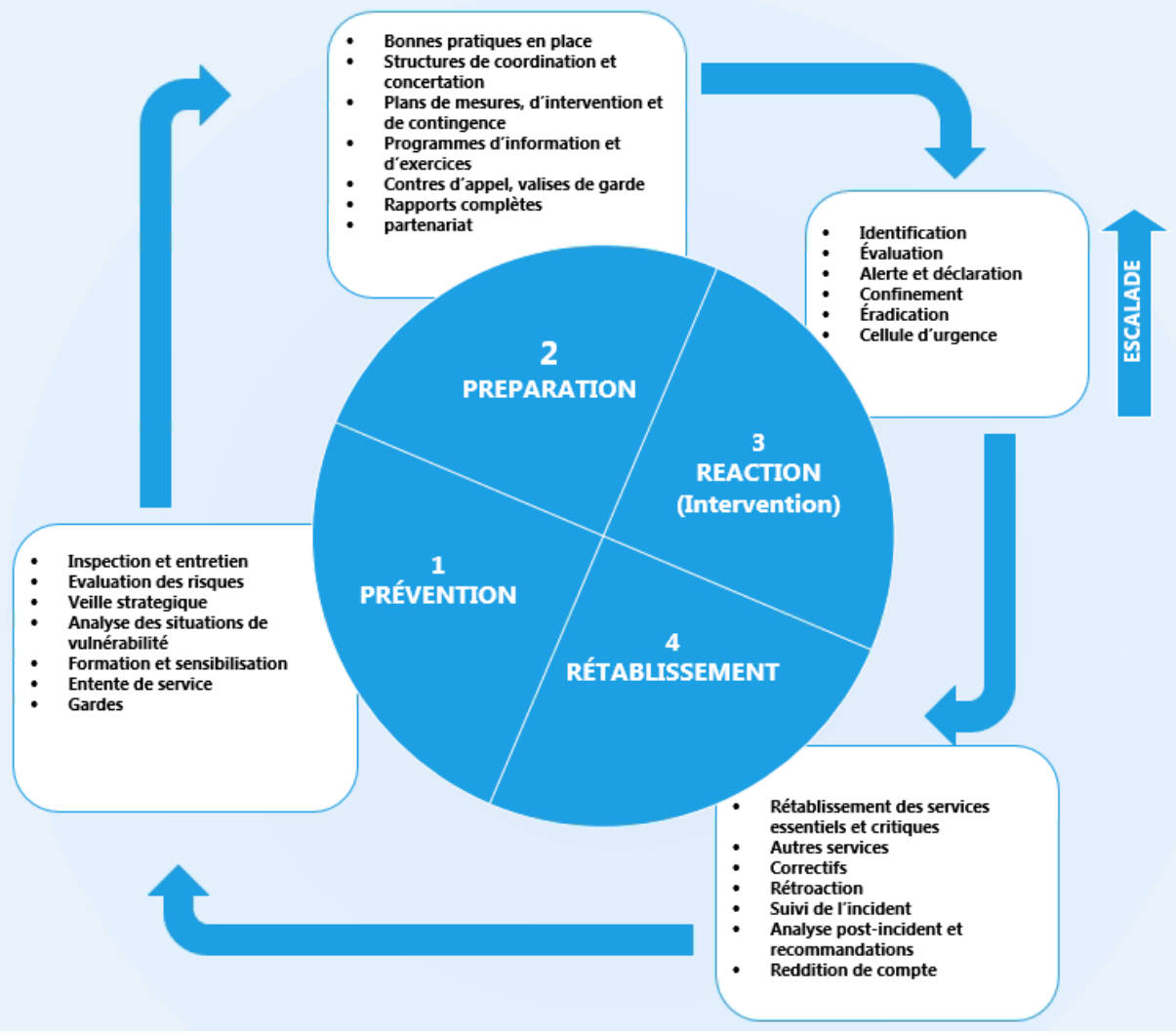

Figure 1 : PROCESSUS DE GESTION DES INCIDENTS DE SÉCURITÉ DE L'INFORMATION DU CIUSSS-EMTL

5.4 LA PRÉVENTION

Le CIUSSS-EMTL met en place des mesures de prévention notamment par l'évaluation périodique des risques, la mise en place d'une stratégie de veille technologique, l'analyse des situations de vulnérabilité et la formation et sensibilisation continue des utilisateurs.

5.4.1 L'INSPECTION ET L'ENTRETIEN

La direction des ressources technologiques (DRT) s'assure de l'inspection physique (équipement) et logique (logiciels, applications) des systèmes d'informations qui sont à sa charge. Elle s'assure aussi de la planification des audits et du suivi des mises à jour des systèmes d'information.

5.4.2 L'ÉVALUATION DES RISQUES

L'évaluation du risque consiste à mettre en relation le niveau de risque, déterminé au cours de l'étape d'analyse, avec les différents éléments issus de l'analyse du contexte organisationnel.

Cette étape revient à faire l'évaluation de l'impact du risque sur la disponibilité, l'intégrité et la confidentialité sur les actifs informationnels.

L'évaluation des risques de sécurité est assurée au CIUSSS-EMTL par l'équipe de sécurité. Elle permet d'identifier le niveau de sévérité de l'évènement et de prévoir la nature du mode d'atténuation approprié à mettre en place.

5.4.3 LA VEILLE STRATÉGIQUE

L'apparition des nouvelles failles de sécurité et les moyens de s'en prémunir doivent être inclus dans la culture du CIUSSS-EMTL.

Le CIUSSS-EMTL met en place un mécanisme de veille informationnelle en vue de favoriser l'aide à la prise de décision stratégique. Cette veille informationnelle constitue une recherche d'informations sur les nouvelles apparitions de vulnérabilités et les nouvelles techniques pour s'en prémunir.

Le MSSS accompagne les établissements dans la gestion et le suivi des traitements d'apparition de nouvelles vulnérabilités. Le réseau de partage (table de concertation des officiers de sécurité (OSI) du RSSS) est toujours à l'écoute des nouveautés en matière de cybersécurité.

5.4.4 L'ANALYSE DES VULNÉRABILITÉS

Au CIUSSS-EMTL, l'analyse des vulnérabilités est assurée par des solutions technologiques. L'analyse de vulnérabilité peut être faite sur plusieurs types de système d'information (applications, réseau vu de l'interne, réseau vu de l'externe, accès physique aux magasins de données, etc.).

Le CIUSSS-EMTL traite sans délai la plupart des vulnérabilités de niveau de criticité élevé, en particulier celles qui pourraient mettre à risque un ou plusieurs processus d'affaires importants ou sensibles.

D'autres vulnérabilités nécessitent moins d'attention, comme celles touchant des infrastructures déjà protégées. Enfin, si l'analyse de vulnérabilité recommande l'installation d'une multitude de mises à jour et de correctifs pour différents logiciels, la correction fera l'objet d'un projet ou d'un changement.

5.4.5 LA FORMATION ET LA SENSIBILISATION

Étant conscient de l'impact humain dans la gestion des risques, le CIUSSS-EMTL met en place une campagne de sensibilisation pour les utilisateurs des systèmes d'information à sa charge.

Pour faire évoluer les comportements individuels des utilisateurs, et afin de mieux faire comprendre les orientations du CIUSSS-EMTL en matière de sécurité de l'information, un processus de sensibilisation est nécessaire. De plus, les intervenants en sécurité de l'information du CIUSSS-EMTL participent à des formations, dont celles offertes par le MSSS.

5.4.6 LES ENTENTES DE SERVICE TECHNOLOGIQUE

Les ententes de service de la DRT stipulent, selon la sévérité de l'événement, les délais de prise en charge et de résolution des incidents. Les équipes opérationnelles de la DRT sont sensibilisées et formées pour prendre en charge les incidents de sécurité dès leur enregistrement dans l'outil de gestion des requêtes.

5.4.7 LA CELLULE D'URGENCE DE LA DRT

La DRT a mis en place une cellule d'urgence pour gérer les alertes de vulnérabilité technologique qui nous viennent du MSSS, plus particulièrement du Coordonnateur organisationnel de la gestion des incidents (COGI). Les membres de la cellule d'urgence se réunissent d'abord pour évaluer l'état de la situation et mettre en place un plan d'action. Par la suite, des experts sont désignés pour faire des suivis d'avancement de chaque étape du plan d'action.

5.4.8 LES GARDES ADMINISTRATIVES ET OPÉRATIONNELLES

Le processus de garde concerne la déclaration d'un incident de sécurité de l'information en dehors des heures de bureau.

Selon la gravité de l'incident de sécurité, la garde opérationnelle en place doit aviser le cadre de garde administratif.

Après l'évaluation de l'évènement, dépendant de la gravité, un processus d'escalade est enclenché. L'évènement est par la suite documenté dans les outils de gestion personnels à chaque garde et assignée à l'OSI.

5.5 LA PRÉPARATION

Aussi efficaces qu'elles puissent être, les mesures de prévention ne peuvent permettre d'éliminer tous les risques. La préparation vise, entre autres, à mettre en place toutes les mesures et les processus requis pour préparer le CIUSSS-EMTL à répondre adéquatement aux incidents de sécurité de l'information, incluant les activités de formation et de sensibilisation à tout le personnel et autres utilisateurs des actifs informationnels[11].

5.5.1 LES BONNES PRATIQUES EN PLACE

Le CIUSSS-EMTL met tout en œuvre pour harmoniser les pratiques dans ses différentes installations. Les règles de bonnes pratiques en place nous proviennent soit des fournisseurs partenaires, soit du MSSS ou encore du réseau de concertation des OSI. Elles sont définies par un ensemble de comportements à adapter pour éviter une situation de non sécurité.

[11] Adapté du PIMUSC du CIUSSS-EMTL, mars 2017, page 67 « Préparation »

5.5.2 LES STRUCTURES DE COORDINATION ET DE CONCERTATION

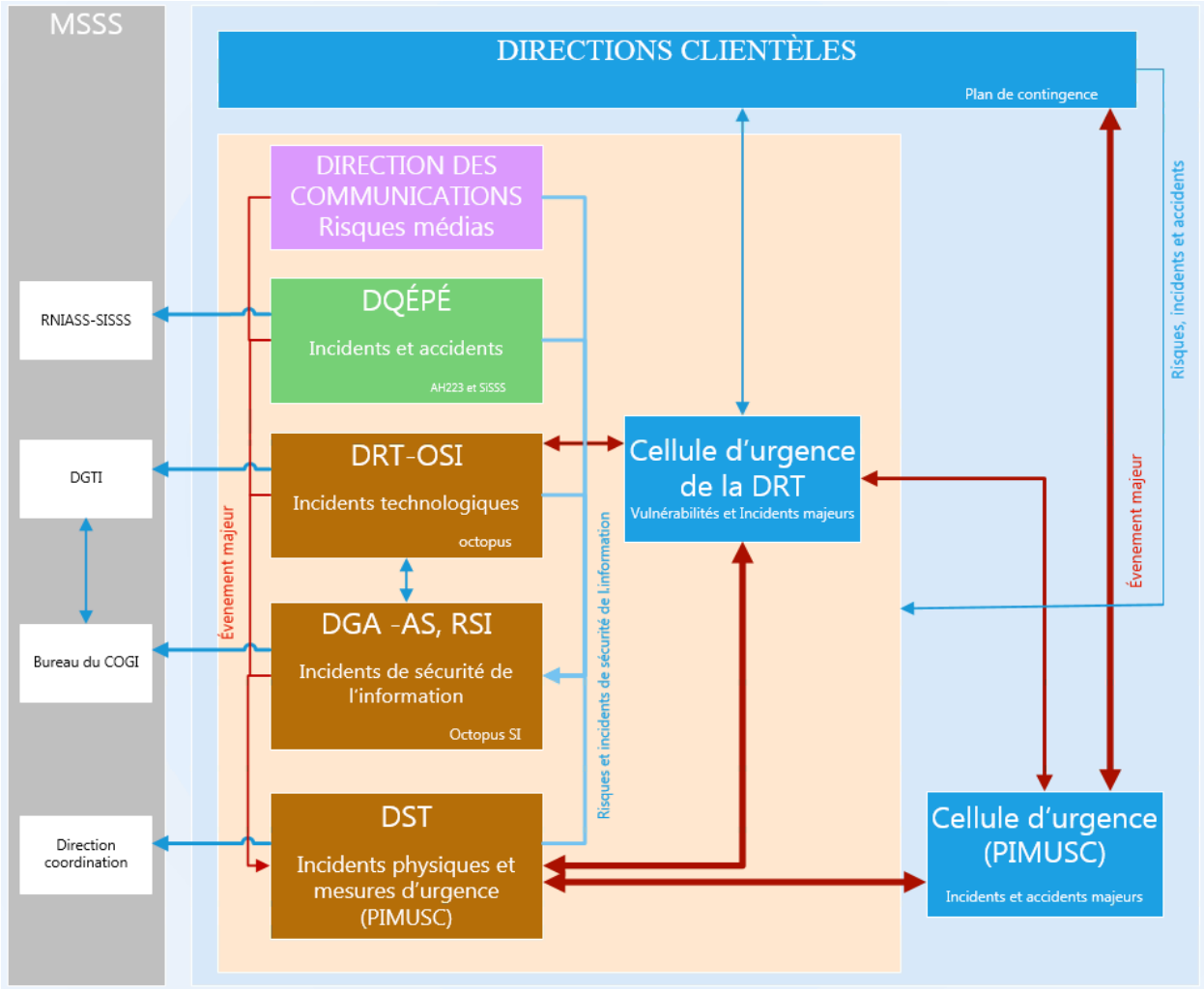

Figure 2 : STRUCTURE DE GESTION DES INCIDENTS DE SÉCURITÉ DE L'INFORMATION DU CIUSSS-EMTL

RNIASS : Registre national des incidents et accidents survenus lors de la prestation de soins

SISSS : Système d'information sur la sécurité des soins et services

DGTI : Direction générale des technologies de l'information

COGI : Conseiller organisationnel de gestion des incidents.

5.5.3 LES PLANS DE MESURES D'INTERVENTION ET DE CONTINGENCE

Les plans de contingences sont élaborés et mis en place par les directions. Le dossier est sous la coordination des mesures d'urgence et de la sécurité civile en lien avec le PIMSC.

5.5.4 LE DÉPLOIEMENT DES MOYENS TECHNOLOGIQUES DE DÉTECTION

La DRT met en place les moyens de détection des incidents technologiques de sécurité de l'information, réels ou potentiels. Les choix des outils de détection sont spécifiques au CIUSSS-EMTL et dépendent de plusieurs facteurs, notamment de l'architecture de sécurité, de l'exposition aux menaces et de la sensibilité de l'information.

Les outils de détections peuvent notamment être :

- le déploiement et la mise à jour de solutions de sécurité (pare-feu et règles de contrôle d'accès, antivirus, anti-logiciel malveillant, etc.);
- l'utilisation d'outils d'analyse des fichiers de journalisation facilitant la détection des accès ou des tentatives d'accès non autorisés ou d'activités inhabituelles;
- la journalisation des accès aux salles de traitement informatique (CTI) et une vérification périodique des accès;
- le déploiement et la gestion d'un système de détection d'intrusion (ex. : installation du système et mise à jour des situations de vulnérabilité et des règles de filtrage)[12].

5.5.5 LES PROGRAMMES D'INFORMATION ET D'EXERCICES

- **LA FORMATION ET LA SIMULATION**

  Le CIUSSS-EMTL s'assure de la formation adaptée aux intervenants et des exercices récurrents de simulation, afin que lors de la réponse à un incident de sécurité de l'information, tous les intervenants comprennent et exécutent, dans les délais requis et de manière appropriée, les tâches qui leur sont confiées.

  Les résultats des exercices sont documentés de façon à mettre en évidence les éventuelles lacunes et incohérences

[12] Pour plus de détails sur ces systèmes, consulter la pratique gouvernementale PR-061 intitulée - Tests d'intrusion et de vulnérabilités

détectées et permettre les ajustements nécessaires au processus par le comité d'amélioration continue.

5.5.6 LES CENTRES D'APPEL ET LES VALISES DE GARDE

Au CIUSSS-EMTL, tous les appels de garde aboutissent au centre d'appel (CDA). Par la suite, l'appel est converti en demande et est transféré à la bonne personne. Si la demande est catégorisée comme un incident de sécurité de l'information, dépendant de son niveau de gravité, le gestionnaire de garde peut être sollicité.

Une valise de garde est mise à la disposition des gestionnaires pour leur période de garde. Cette valise est un outil de support qui renferme de l'information et des processus pour aider le gestionnaire dans l'accomplissement de ses tâches et pour le support à la décision.

5.5.7 LA RÉVISION DES RAPPORTS COMPLÉTÉS (ANTÉRIEURS)

Documentation des incidents afin d'en faire un suivi administratif dans un processus d'amélioration continue des procédures et des politiques en place.

5.5.8 LA FORMATION DE COMITÉS

Dans le cadre de la gestion des incidents, des comités sont formés afin d'adresser différents types d'incidents. Ces comités sont sous la responsabilité du coordonnateur des mesures d'urgence de la DST.

5.6 LA RÉACTION (OU INTERVENTION)

Le CIUSSS-EMTL déploie des processus et plans d'action préétablis, un ensemble de stratégies et de mesures afin de répondre à un incident de sécurité de l'information rapidement et adéquatement. La réaction à l'événement vise à assurer la protection des personnes et des actifs informationnels du CIUSSS-EMTL.

5.6.1 L'IDENTIFICATION DE L'INCIDENT OU DU RISQUE

Les moyens de détection et d'actions de surveillance sont mis en place afin d'identifier un incident de sécurité de l'information.

5.6.2 LA DÉCLARATION D'UN INCIDENT OU DU RISQUE

Tout utilisateur des actifs informationnels du CIUSSS-EMTL a l'obligation, tel que stipulé dans la Politique de sécurité de l'information du CIUSSS-EMTL (POL-024), de signaler immédiatement tout acte ou situation dont il a connaissance susceptible de constituer une violation réelle ou présumée des règles de sécurité, ainsi que toute anomalie pouvant nuire à la protection des actifs informationnels du CIUSSS-EMTL.

5.6.3 LA PROCÉDURE DE DÉCLARATION DES INCIDENTS OU RISQUES DE SÉCURITÉ DE L'INFORMATION[13]

Au CIUSSS-EMTL, la déclaration des risques doit se faire auprès des acteurs de la sécurité, principalement par les méthodes suivantes :

- Aviser son supérieur de l'événement ou, si le contexte ne le permet pas, aviser alors le responsable de la sécurité de l'information (RSI) du CIUSSS-EMTL;
- Ou, dans le cas d'un contractant externe, aviser son employeur ou le responsable du CIUSSS-EMTL auquel il se rapporte;
- Et obligatoirement compléter une déclaration d'incident ou d'accident à l'aide du formulaire décrit à l'annexe 1. Si l'événement est survenu lors d'une prestation de soins et de services aux usagers, compléter le formulaire AH-223.

5.6.4 LA CONFIDENTIALITÉ DES DOSSIERS DE DÉCLARATION

Toutes les déclarations ou requêtes de sécurité de l'information sont traitées confidentiellement par l'équipe de sécurité de l'information du CIUSSS-EMTL DRT, en autant que la déclaration ou la requête soit acheminée selon la procédure de déclaration mentionnée au point 5.6.3 et incluse à la Politique POL-024 disponible sur Intranet.

5.6.5 LA DÉTECTION DES INCIDENTS ET RISQUES

La détection des risques et des incidents de sécurité de l'information, réels ou potentiels, se fait au moyen d'outils de détection technologiques ou par les autres moyens de détection mis en place (voir la rubrique 5.5 La préparation).

5.6.6 LA SURVEILLANCE

Les actions de surveillance suivantes sont mises en place pour la détection d'un incident de sécurité de l'information :

- journalisation et surveillance des accès, qu'ils soient physiques (exemples : accès aux locaux, aux équipements et aux infrastructures de communication) ou logiques (ex. : accès ou tentatives d'accès à l'information via le réseau informatique du CIUSSS-EMTL);

- examen régulier de rapports automatisés sur la performance des systèmes en vue d'y déceler d'éventuelles activités suspectes;

[13] Voir le Formulaire de déclaration d'incident de sécurité de l'information

- contrôle régulier de l'application de mesures administratives (application de politiques et de procédures, sensibilisation du personnel, etc.).

5.6.7 L'ÉVALUATION DE L'INCIDENT OU DU RISQUE

L'instance responsable et l'équipe de sécurité de l'information évaluent l'incident ou le risque de sécurité de l'information afin de déterminer notamment :

- la classification de l'incident de sécurité de l'information;
- le niveau de sévérité d'un tel incident;
- les systèmes affectés;
- l'impact sur la disponibilité, l'intégrité et la confidentialité des données;
- l'impact sur la prestation de services;
- l'impact sur le respect des droits fondamentaux à la protection des renseignements personnels et de la vie privée;
- les pertes financières rattachées à un tel incident;
- la recherche et l'analyse des preuves nécessaires à la conduite d'une enquête (voir la rubrique 5.9) qui pourrait être déclenchée dès la détection de l'incident.

5.6.8 LA PRÉSERVATION DES PREUVES

L'évaluation de l'incident permet également la recherche et l'analyse des preuves nécessaires à la conduite d'une enquête (voir section 5.4 La prévention) qui pourrait être déclenchée dès la détection de l'incident de sécurité de l'information.

5.6.9 LE PROCESSUS D'ESCALADE (alerte aux instances)

Le CIUSSS-EMTL met en place un ensemble de procédures prédéfinies en vue de recourir aux services des spécialistes ou à un palier de décision supérieur lors d'un événement indésirable. Le processus d'escalade doit être enclenché dès la détection des incidents de sévérité critique ou importante. Ce processus est approuvé par la haute direction et communiqué aux intervenants concernés.

Le processus d'escalade dépend des niveaux de sévérité d'un tel incident :

- les incidents de niveaux bas, modérés et importants doivent être gérés au sein du réseau en fonction de leur niveau de sévérité;

- le CIUSSS-EMTL a l'obligation d'escalader les incidents à portée gouvernementale (niveau critique) au COGI dans les plus brefs délais afin que les actions appropriées puissent être prises par les intervenants concernés. Le tableau suivant détaille les modalités d'escalade afin de coordonner les interventions administratives et opérationnelles.

Figure 3 : GRILLE D'ESCALADE DES INCIDENTS

Sévérité	Officier de sécurité OSI (CIUSSS-EMTL)	RSI et le directeur de la DRT	COGI (MSSS)	DRT[14] (MSSS)	DPI[15] (SCT)	DRT cellule d'urgence
Critique	Averti immédiatement	Averti immédiatement	Averti immédiatement	Averti immédiatement via la cellule d'urgence du RSSS	Processus de gestion des incidents à portée gouvernementale	Processus de gestion de cellule d'urgence
Importante	Averti immédiatement	Averti immédiatement	Averti immédiatement	Informé biannuellement via le tableau de bord RSSS	Via le bilan annuel de sécurité	Processus de gestion de cellule d'urgence
Modérée	Informé annuellement	Informer à la quinzaine (statutaire)	Informé annuellement	Informé via le bilan annuel de sécurité	s.o.	s.o.
Basse		Informer à la quinzaine (statutaire)			s. o.	s.o.

Un formulaire de déclaration des incidents de sécurité de l'information est présenté à l'annexe 1. Également, la présente politique est appuyée par un outil « Grille d'escalade des incidents », sous forme de chiffrier Excel, représentant les modalités d'escalade, advenant un tel incident.

5.6.10 LES MESURES D'URGENCE

À la suite d'un évènement, l'alerte est envoyée aux cadres supérieurs par message texte avec une demande de confirmation et s'il y a lieu dépendant du niveau de gravité, une cellule d'urgence est mise en place.

[14] Dirigeant du réseau de l'information (MSSS)
[15] Dirigeant principal de l'information (Secrétariat du conseil du Trésor)

5.6.11 LE CONFINEMENT DES DOMMAGES

Une fois l'incident de sécurité de l'information détecté et analysé, les activités permettant de le contenir sont immédiatement enclenchées en vue d'en limiter les dommages pour le CIUSSS-EMTL. Les activités de confinement se caractérisent par leur rapidité d'exécution. Elles peuvent, selon la nature d'un tel incident, se traduire notamment par le renforcement des mesures de sécurité (isoler une ou plusieurs composantes de l'infrastructure technologique, modification des règles de contrôle d'accès physique ou logique), la mise hors service d'un serveur affecté, la modification des règles de filtrage d'un pare-feu ou d'un routeur, ou la désactivation d'un service.

Le CIUSSS-EMTL élabore une stratégie prédéfinie concernant la décision de recourir aux activités de confinement. Cette stratégie tient compte des risques acceptables par le CIUSSS-EMTL, en raison de ses conséquences sur les systèmes de mission de l'organisation. Les stratégies de confinement varient selon la classification de l'incident de sécurité de l'information.

Les stratégies de confinement sont élaborées séparément pour chaque type d'incident de sécurité de l'information et portées à la connaissance des intervenants chargés de leur mise en œuvre. Ces stratégies devront tenir compte, notamment :

- des conséquences potentielles;
- du besoin de préserver des preuves;
- de la disponibilité des services (connectivité réseau, services fournis à la clientèle interne et externe, etc.);
- du temps et des ressources nécessaires à la mise en œuvre de la stratégie retenue;
- de l'efficacité de la stratégie (confinement total ou partiel).

5.6.12 L'ÉRADICATION DU PROBLÈME

Une fois l'incident de sécurité de l'information confiné et les dommages contenus, l'étape d'éradication vient éliminer la cause de cet incident en corrigeant les situations de vulnérabilité, en y apportant des correctifs ou en éradiquant la source de l'incident.

Le CIUSSS-EMTL met en place des procédures préétablies pour l'étape d'éradication, qui permettent de s'assurer qu'aucun détail n'a

été omis. La complexité de ces procédures varie selon la nature et la sévérité de l'incident de sécurité de l'information.

Une attention toute particulière est accordée à cette étape lors de la conduite d'une enquête, notamment en ce qui a trait à la préservation des preuves.

5.7 LE RÉTABLISSEMENT DES ACTIVITÉS ET SERVICES

Le CIUSSS-EMTL met en place un ensemble d'actions visant à soutenir le retour à la normale de ses activités et services à la suite d'un événement indésirable. Le rétablissement consiste essentiellement à mettre en place les mesures et les modalités visant à assurer le retour graduel à des conditions normales des activités et services touchés par l'incident de sécurité de l'information[16].

5.7.1 LE RÉTABLISSEMENT DES SERVICES ESSENTIELS ET CRITIQUES ET LE RÉTABLISSEMENT DES AUTRES SERVICES

Le CIUSSS-EMTL rétablit progressivement les services, une fois l'incident de sécurité de l'information traité et sa cause éliminée, en accordant la priorité à ceux identifiés comme étant critiques pour l'organisation.

5.7.2 LES CORRECTIFS À LA SITUATION

Pour rétablir un système après un incident, le CIUSSS-EMTL applique les correctifs qui sont nécessaires. Ces correctifs sont installés en vue de prévenir l'incident (mode proactif ou préventif) ou pour corriger un événement indésirable (mode réactif).

5.7.3 LA RÉTROACTION

La rétroaction étant une étape très importante pour la gestion des incidents, elle est utilisée au CIUSSS-EMTL afin de revoir l'événement dans son ensemble et de planifier un plan d'action pour les risques résiduels.

Le CIUSSS-EMTL, au cours de la rétroaction, assure aussi la décision de réviser la solution à mettre en place pour éviter l'apparition des incidents futurs.

5.8 LE BILAN

Les intervenants du CIUSSS-EMTL doivent conserver toute documentation se rapportant à l'incident de sécurité de l'information, tel que le suivi de l'incident, l'analyse post-incident et la recommandation, la révision du processus et la reddition de compte aux instances. De plus, les intervenants

[16] Adapté du PIMUSC du CIUSSS-EMTL, mars 2017, page 68 « Rétablissement »

du CIUSSS-EMTL doivent mettre à jour les politiques et les procédures en vigueur dans l'organisation.

5.9 LA CONDUITE D'ENQUÊTE

Bien qu'elle ne soit pas toujours requise, certains incidents de sécurité de l'information, potentiels ou réels, peuvent rendre indispensable la tenue d'une enquête, menée par le secteur responsable selon nos structures internes, par une équipe indépendante ou par la Sûreté du Québec, en raison de ses responsabilités horizontales comme énoncées dans le Cadre gouvernemental de gestion de la sécurité de l'information. À cet égard, la collecte et la préservation des éléments de preuves nécessaires à l'enquête sont effectuées dès détection d'un tel incident.

Durant la conduite d'une enquête, les principes suivants sont respectés :

- les preuves sont préservées, recueillies, conservées et analysées;
- les conclusions sont appuyées par des faits et des preuves;
- l'enquête est complète, indépendante et exempte de contraintes et influences extérieures;
- la confidentialité est assurée.

Le dossier d'enquête est généralement constitué d'un rapport d'enquête, d'enregistrements de diverses natures, de copies de banques de données, de notes prises lors d'entrevues, de preuves, etc. Ces éléments sont conservés conformément à leur calendrier de conservation.

6 RÔLES ET RESPONSABILITÉS

6.1 Le président-directeur général

Dans le cadre de gestion des incidents, le président-directeur général du CIUSSS-EMTL a notamment les responsabilités suivantes :

- veiller à la mise en œuvre du processus de gestion des incidents de sécurité de l'information;
- assurer le suivi de l'évolution de la prise en charge des incidents;
- convoquer la cellule d'urgence et en assurer la présidence;
- examiner les recommandations qui lui sont formulées, procéder à leur diffusion et en assurer le suivi de la mise en œuvre;
- s'assurer de la formation des intervenants à l'identification des incidents de sécurité de l'information et des parties prenantes au processus pour une meilleure exécution des tâches qui leur sont confiées;

- assurer la responsabilité des communications avec les médias.

6.2 La direction générale adjointe – Administration et soutien (DGA-AS)

La DGA-AS est responsable de valider le contenu de la présente politique de sécurité de l'information et de la présenter au comité de direction pour approbation.

6.3 Le comité de direction

Le comité de direction adopte les politiques de sécurité de l'information établies par le CIUSSS-EMTL et ses mises à jour, et en suit l'application.

6.4 La cellule d'urgence de la DRT

Dans le cadre de la gestion des incidents de sécurité de l'information, la cellule d'urgence est celle déterminée par le Programme d'intervention des mesures d'urgence et sécurité civile (PIMUSC) sous la responsabilité de la DST. La composition et le mode de fonctionnement de la cellule d'urgence sont déterminés dans le PIMUSC du CIUSSS-EMTL.

Le rôle de la cellule d'urgence se décline comme suit, en regard des incidents majeurs de sécurité de l'information :

- Prendre des décisions de nature stratégique;
- Évaluer l'impact de l'incident sur les activités du CIUSSS-EMTL et éventuellement son impact sur d'autres organismes;
- Établir un plan d'intervention, en assurer le suivi et les ajustements;
- Formuler des recommandations;
- Mobiliser les ressources nécessaires à la mise en œuvre du plan d'intervention (ressources humaines, financières et matérielles);
- Émettre les politiques et procédures nécessaires et s'assurer de leur application;
- Superviser le rétablissement des activités, après un incident.

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

Il veille à la communication, à la compréhension et l'application par les principaux intervenants, les autres responsables désignés et les utilisateurs, des politiques de sécurité de l'information du CIUSSS-EMTL.

Dans le cadre de gestion des incidents, il a notamment les responsabilités suivantes :

- s'assurer de la mise en œuvre du processus de gestion des incidents de sécurité de l'information au sein du CIUSSS-EMTL;
- assurer le suivi de la prise en charge des incidents;

- déclarer un incident de sécurité de l'information au COGI si le niveau de sévérité « critique » ou « important » est atteint, selon les modalités fixées par le DRI du MSSS;
- mettre en place une équipe d'intervention opérationnelle apte à prendre en charge et traiter les incidents de sécurité de l'information;
- convoquer la cellule d'urgence de la DRT, sur proposition de l'OSI et du conseiller en gouvernance de la sécurité de l'information lorsque les tentatives de réponse à un tel incident sont infructueuses et que le niveau de sévérité « critique » est atteint;
- transmettre annuellement au DRI du MSSS ou à son représentant le bilan des incidents de sécurité de l'information, selon les modalités fixées par le DRI.

6.6 Le conseiller en gouvernance de la sécurité de l'information (CGSI)

Dans le cadre de la gestion des incidents de sécurité de l'information, il a notamment les responsabilités suivantes :

- mettre en œuvre le processus de gestion des incidents de sécurité de l'information;
- assurer le suivi de l'évolution de la prise en charge des incidents;
- contribuer, conjointement avec l'OSI, à l'évaluation du niveau de sévérité des incidents ainsi qu'à leur classification selon les échelles reconnues par le DRI du MSSS;
- apporter son soutien et son expertise au RSI;
- répondre aux demandes de soutien de l'OSI dans la prise en charge d'un incident;
- informer le RSI d'un incident de sécurité de l'information et de l'évolution de sa prise en charge;
- émettre, si nécessaire, un bulletin de sécurité à l'endroit des membres du réseau d'alerte gouvernemental leur signalant les vulnérabilités et les mesures à prendre afin de réduire les risques associés;
- planifier, organiser, de coordonner et assurer le suivi des exercices de simulation du processus gouvernemental de gestion des incidents;
- tenir à jour le registre global des incidents de sécurité de l'information et en assurer la gestion.

6.7 L'officier de sécurité (OSI)

Dans le cadre de la gestion des incidents, il a notamment les responsabilités suivantes :

- identifier un incident technologique de sécurité de l'information et le déclarer au RSI;

- contribuer, conjointement avec le CGSI, à l'évaluation du niveau de sévérité de l'incident ainsi qu'à sa classification selon les échelles reconnues par le DRI du MSSS;
- procéder au traitement de l'incident technologique de sécurité de l'information;
- coordonner les travaux de l'équipe technologique d'intervention opérationnelle, advenant un incident de sécurité de l'information;
- répondre aux demandes de soutien des utilisateurs ou du centre de support informatique (CSI) dans la prise en charge d'un incident;
- émettre, si nécessaire, un bulletin de sécurité à l'endroit des membres du réseau d'alerte gouvernemental leur signalant les vulnérabilités et les mesures à prendre afin de réduire les risques associés;
- siéger à la cellule d'urgence, sur invitation du RSI;
- réaliser l'analyse post-incident pour le volet technologique;
- appliquer les recommandations découlant de l'analyse post-incident, pour le volet technologique;
- maintenir à jour les composantes du processus de gestion des incidents de sécurité de l'information (liste des contacts, procédures et modalités de communication, etc.);
- tenir à jour le registre des incidents technologiques de sécurité de l'information et en assurer la gestion;
- planifier, organiser, coordonner et assurer le suivi des exercices de simulation du processus gouvernemental de gestion des incidents.

6.8 La direction des Ressources technologiques (DRT)

La DRT est responsable d'émettre les procédures complémentaires à la présente politique, pour le volet technologique, et de veiller à la gestion et à la prise en charge des activités qui la concerne, découlant de cette politique.

6.9 La direction de la Qualité, de l'évaluation, de la performance et de l'éthique (DQÉPÉ)

Dans le cadre de la gestion des incidents de sécurité de l'information touchant les usagers du CIUSSS-EMTL, à la suite d'une déclaration d'incident ou de risque de sécurité de l'information (AH-223), la DQÉPÉ a la responsabilité d'alerter le RSI du CIUSSS-EMTL et d'assurer conjointement le suivi de l'événement, ainsi que sa déclaration aux instances requises du MSSS.

6.10 Les directions des Ressources humaines, des communications et des affaires juridiques (DRHCAJ), de l'Enseignement universitaire, de la Recherche et de la Logistique

Elles sont responsables, notamment, d'informer tout nouveau gestionnaire ou employé œuvrant au sein du CIUSSS-EMTL ou tout nouveau fournisseur ou partenaire du CIUSSS-EMTL, sous leur responsabilité, dès son accueil ou le début de son mandat, de ses obligations découlant des politiques en vigueur en matière de sécurité de l'information. Plus particulièrement, la DRHCAJ doit s'assurer de fournir et d'offrir aux gestionnaires le soutien et l'assistance requise quant au respect de la présente politique.

La DRHCAJ veille également au respect de la confidentialité des informations et à la protection des renseignements personnels notamment, au respect et à l'application conforme des règles entourant la confidentialité de ces informations prévues à la LSSSS et à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ c A-2.1. Elle s'assure notamment du respect de la confidentialité des informations diffusées sur ses propres médias ou outils d'information (sites Internet, réseaux sociaux, Info-Lettre, etc.) Elle forme et accompagne les porte-paroles identifiés par l'organisation afin de s'assurer de l'intégrité des informations diffusées.

6.11 Les directions

Elles sont responsables de l'élaboration et de la mise en place de leur plan de contingence. Elles sont aussi responsables de la mise en œuvre, auprès de tout gestionnaire œuvrant au sein du CIUSSS-EMTL et relevant de leur autorité, des dispositions de la présente politique de gestion des incidents de sécurité de l'information du CIUSSS-EMTL.

6.12 La direction des Services techniques (DST)

Dans le cadre de gestion des incidents, la DST a notamment les responsabilités suivantes :

- Assurer le suivi des incidents de sécurité de l'information relevant de son domaine d'intervention (accès aux locaux, sinistres physiques, etc.);
- Élaborer, mettre en œuvre et mettre à jour le Plan intégré de mesures d'urgence et de sécurité civile (PIMUSC) du CIUSSS-EMTL;
- Déclencher les mesures d'urgences et réunir la cellule d'urgence;
- Par l'application du PIMUSC, soutenir le maintien des services essentiels et critiques en cas de sinistre, entre autres en coordonnant le déclenchement des plans de contingences et de relève des différentes directions du CIUSSS-EMTL, incluant la DRT.

6.13 Les utilisateurs

Tel que stipulé à la politique de sécurité de l'information du CIUSSS-EMTL (POL-024), les utilisateurs ont l'obligation de se conformer aux politiques et procédures du CIUSSS-EMTL en matière de sécurité de l'information.

Ils ont également l'obligation de signaler immédiatement selon la procédure de déclaration des incidents de sécurité de l'information, mentionnée à la section 5.6.3, tout acte ou situation dont ils ont connaissance et susceptible de constituer une violation réelle ou présumée des règles de sécurité, ainsi que toute anomalie pouvant nuire à la protection des actifs informationnels du CIUSSS-EMTL.

7 ÉLABORATION, RÉDACTION ET MISE À JOUR DE LA POLITIQUE

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

Le RSI est responsable de l'élaboration, de la rédaction et de la mise à jour de la politique.

7.2 Comité de sécurité de l'information

Les membres du comité de sécurité de l'information ont participé à la validation de la politique et participent à la validation de sa mise à jour.

7.3 Calendrier de révision de la politique

La présente politique devra être révisée tous les 4 ans ou plus rapidement en fonction des besoins.

8 RESPONSABLE DE LA MISE EN APPLICATION

8.1 Le responsable de la sécurité de l'information (RSI) du CIUSSS-EMTL

Il est responsable de la mise en application de la présente politique.

9 ENTRÉE EN VIGUEUR

La présente politique entre en vigueur le jour de son adoption par le comité de direction et annule, par le fait même, toute autre politique en cette matière adoptée antérieurement dans l'une ou l'autre des installations administrées par le CIUSSS-EMTL.

10 ANNEXE(S)

- ANNEXE 1 – Formulaire de déclaration d'incident de sécurité de l'information

Centre intégré universitaire de santé et de services sociaux de l'Est-de-l'Île-de-Montréal
Québec

ANNEXE 1

Formulaire de déclaration d'incident de sécurité de l'information

au MSSS par l'équipe de sécurité (Formulaire du MSSS)

FORMULAIRE DE DÉCLARATION D'INCIDENT DE SÉCURITÉ		
Numéro de l'incident : **Titre abrégé de l'incident :** **Nom de l'organisme :**		**Date d'ouverture :** **Date & heure de l'incident :** **Durée :**
Souligné par :		**Téléphone :**
Site(s) impacté(s) :	**Secteur(s) affecté(s) :**	**Actif(s) affecté(s) et catégorisation** Nom de l'actif D-I-C

Description sommaire de l'incident et des actions réalisées : (mettre en référence les analyses, rapports ou journaux et les copier dans le répertoire associé au billet)

Date	Heure	Actions réalisées / Situation

Classification selon MSSS-DIR01[6]		Classe d'incidents selon RP- Déclaration incidents[7]-DSQ		Sévérité MSSS-DIR01	
1. Atteinte sécurité physique	☐	Atteinte sécurité physique	☐	1. Basse	☐
2. Code malicieux	☐	Code malicieux	☐	2. Modérée	☐
3. Comportement inapproprié	☐	Usage inapproprié	☐		
		Infraction Code civil, LSSSS, LPCRS	☐	3. Importante *	☐
		Infraction au Code criminel	☐		
4. Cyberattaque	☐	Déni de service	☐	4. Critique *	☐
5. Dysfonctionnement technologique	☐	Fonctionnement inadéquat	☐		
6. Vol ou perte d'information	☐	Bris de confidentialité	☐	*Le RSI, l'officier de sécurité et le COGI doivent être avisés	
		Destruction/modif. non autorisée	☐		
Autres			☐		

Description des impacts / conséquences Impacts sur la clientèle : Oui ☐ Non ☐

Cause(s):

Lacune(s) décelée(s)

Plan de communication et escalade

Date	Heure	Groupe, fonction ou instance visés	Sommaire du message