TABLE DES MATIERES

Pour copie papier seulement : *Le document original est approuvé avec signature numérique sous la responsabilité de l'AQ.*

1. But

> Cette politique vise à communiquer les engagements d'HÉMA-QUÉBEC à l'égard de la gestion de ses risques de cybersécurité ainsi que ceux reliés aux actifs informationnels, tels que :

- La perte de la disponibilité, de l'intégrité et/ou de la confidentialité des actifs informationnels;
- L'atteinte à la vie privée des individus;
- La non-conformité aux lois et règlements applicables.

2. Portée et champ d'application

> La présente politique s'applique aux utilisateurs, actifs, activités et situations suivants :

- À l'ensemble du personnel d'HÉMA-QUÉBEC qui utilise ou accède aux informations détenues par HÉMA-QUÉBEC dans le cadre de leurs fonctions ainsi qu'aux intervenants externes, fournisseurs de services ou tiers mandatés par HÉMA-QUÉBEC;
- À toute personne physique ou morale qui utilise ou accède, par le réseau d'HÉMA-QUÉBEC, à des informations confidentielles, ou non, quel que soit le support sur lequel ces informations sont conservées et quel que soit le lieu. Afin de simplifier la lecture du texte, le terme « utilisateur » remplace et inclut tout ce qui précède;
- À l'ensemble des actifs informationnels, ainsi qu'à leur utilisation, qu'HÉMA-QUÉBEC détient dans l'exercice de sa mission tels que les banques d'information, les informations et les données sans égard aux médiums de support ou son moyen de communication, les réseaux, les systèmes d'information, les logiciels, les équipements informatiques ou centres de traitement utilisés par HÉMA-QUÉBEC; et ce, tout au long de leur cycle de vie;
- À l'ensemble des activités de collecte, d'enregistrement, de traitement, de sauvegarde, de transmission, de conservation, de destruction et de diffusion des actifs informationnels d'HÉMA-QUÉBEC;
- Aux centres de données, bureaux, salles et autres emplacements de travail (incluant les collectes mobiles) d'HÉMA-QUÉBEC;
- À toute situation qui pourrait permettre de voir ou d'entendre des informations à caractère confidentiel de façon accidentelle ou non.

3. Définitions

> **Actif informationnel** : une banque d'informations, 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.

- **Actif informationnel critique** : un actif informationnel nécessaire à l'exécution d'un processus critique dont un bris de disponibilité, d'intégrité ou de confidentialité peut impacter d'une façon significative l'atteinte des objectifs stratégiques de l'organisation.
- **Cycle de vie** : Période de temps couvrant toutes les étapes d'existence de l'information ou de l'actif informationnel, dont celles (selon la terminologie) de la définition, de la création, de l'enregistrement, du traitement, de la diffusion, de la conservation et de la destruction.
- **Détenteur d'actifs informationnels** : Gestionnaire désigné comme responsable de l'actif informationnel nécessaire à la conduite des activités de l'entreprise.
- **Mesure de sécurité** : 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 d'apparition de ces risques ou à réduire les pertes qui en résultent.
- **Registre des autorités** : Répertoire, recueil ou fichier, dans lequel sont inscrites les désignations effectuées et les délégations consenties aux fins de la gestion de la sécurité, ainsi que les responsabilités qui y sont rattachées.
- **Renseignement (information) confidentiel(le)** : Donnée ou information désignée confidentielle par une loi, un règlement ou l'organisation, à laquelle seules les personnes dûment autorisées peuvent avoir accès ou dont la communication et la diffusion sont limitées aux seules personnes ou entités dûment autorisées.
- **Renseignements personnels** : Renseignements concernant une personne physique et permettant de l'identifier. Le nom d'une personne physique n'est pas un renseignement personnel, sauf lorsqu'il est mentionné avec un autre renseignement la concernant ou lorsque sa seule mention révélerait un renseignement personnel concernant cette dernière.

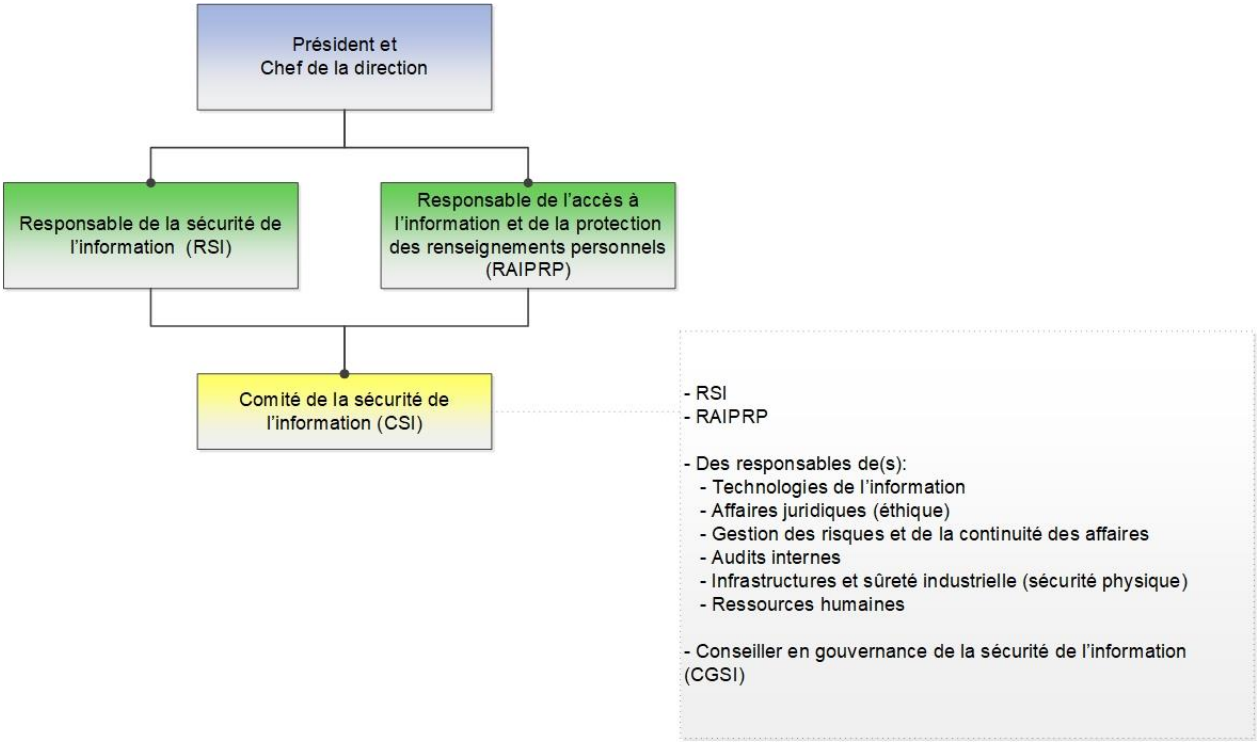
4. Cadre juridique et normatif

- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, LRQ, c A-2.1;
- Règlement sur la diffusion de l'information et sur la protection des renseignements personnels;
- MSSS-CDG01 Cadre de gestion de la sécurité de l'information 17-08-2015 du ministère de la Santé et des Services sociaux.

5. Rôles et responsabilités

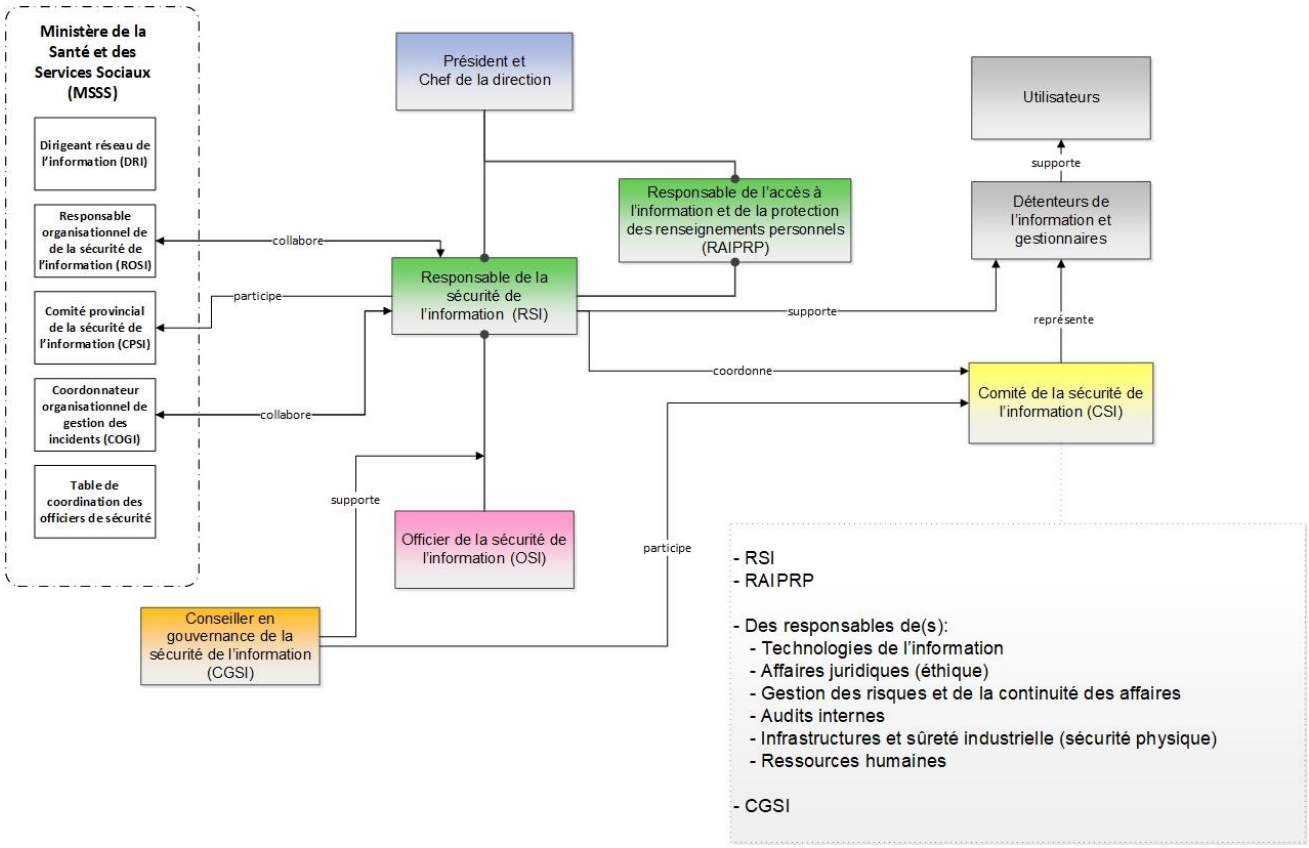
5.1. STRUCTURE DE COORDINATION DE LA SÉCURITÉ DE L'INFORMATION

> La structure interne de coordination en matière de sécurité de l'information mise en place est la suivante :



5.2. STRUCTURE FONCTIONNELLE DE LA SÉCURITÉ DE L'INFORMATION

> La structure fonctionnelle de la sécurité de l'information est illustrée dans le schéma suivant :



5.2.1. PRÉSIDENT ET CHEF DE LA DIRECTION

> Il s'assure principalement :

- Du respect des lois et des règles de sécurité de l'information;
- D'approuver la présente et d'en assurer l'application;
- D'apporter les appuis financiers et logistiques nécessaires pour la mise en œuvre et l'application de la présente politique;
- De la mise en place d'un comité chargé de la sécurité de l'information au sein de son organisation et mandate le responsable de la sécurité de l'information (RSI) et le responsable de l'accès à l'information et de la protection des renseignements personnels (RAIPRP) pour co-présider ce comité;
- De soumettre le bilan annuel concernant l'application de la politique au conseil d'administration;

- D'exercer son pouvoir d'enquête et d'appliquer les sanctions prévues à la présente politique, lorsque nécessaire;
- De nommer un responsable de la sécurité de l'information pour le représenter en cette matière dans l'organisation et pour la réalisation de l'ensemble des mesures précitées.

5.2.2. RESPONSABLE DE LA SÉCURITÉ DE L'INFORMATION (RSI)

> Assiste le président dans la détermination des orientations stratégiques et des priorités d'intervention et préside conjointement avec le RAIPRP le comité de la sécurité de l'information.

> Planifie et dirige la coordination et la cohérence des activités nécessaires à la mise en place de la sécurité de l'information au sein d'HÉMA-QUÉBEC, notamment celles de son officier de sécurité de l'information et de son conseiller en gouvernance de la sécurité.

5.2.3. RESPONSABLE DE L'ACCÈS À L'INFORMATION ET DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS (RAIPRP)

> Le président et chef de la direction d'HÉMA-QUÉBEC désigne un Responsable de l'accès à l'information et de la protection des renseignements personnels (RAIPRP) à qui il délègue les fonctions qui lui sont conférées par la Loi sur l'accès aux organismes publics et sur la protection des renseignements personnels.

> Le RAIPRP assiste le président et chef de la direction dans la mise en œuvre des responsabilités et obligations qui découlent du Règlement sur la diffusion de l'information et sur la protection des renseignements personnels et préside conjointement avec le RSI le comité de la sécurité de l'information en ce qui concerne l'accès aux informations et à la protection des renseignements personnels. Le rôle du RAIPRP est sous la responsabilité de la Vice-présidence Secrétariat général, risques et audits.

5.2.4. CONSEILLER EN GOUVERNANCE DE LA SÉCURITÉ DE L'INFORMATION (CGSI)

> Le Conseiller en gouvernance de la sécurité de l'information (CGSI) apporte son soutien au RSI, notamment en ce qui concerne l'encadrement de la sécurité de l'information, le choix des moyens pour répondre aux exigences des règles particulières adoptées par le Dirigeant réseau de l'information (DRI) et la planification des actions en sécurité.

5.2.5. OFFICIER DE SÉCURITÉ DE L'INFORMATION (OSI)

> L'Officier de sécurité de l'information (OSI) est un professionnel de la sécurité de l'information. Il supporte le RSI et le CGSI dans les activités opérationnelles de sécurité de l'information.

> Il 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 à HÉMA-QUÉBEC, 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.

5.2.6. RESPONSABLE DE LA GESTION DES TECHNOLOGIES DE L'INFORMATION

> La direction Infrastructures et opérations TI est responsable d'agir en tant que fournisseur de service à l'égard de la sécurité des actifs informationnels. Elle fournit et maintient en état les moyens techniques de sécurité et s'assure de leur conformité aux besoins de sécurité, déterminés par le RSI et les détenteurs.

5.2.7. DÉTENTEURS D'ACTIFS INFORMATIONNELS

> Les détenteurs d'actifs informationnels sont responsables d'assurer la sécurité d'un ou de plusieurs actifs informationnels qui leur sont confiés par le responsable de la sécurité de l'information ou un tiers mandaté. À cet égard, ils :
>
> - 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;
> - S'assurent que les mesures de sécurité appropriées sont élaborées, approuvées, mises en place et appliquées systématiquement;
> - S'assurent que leur nom est consigné dans le registre des autorités (pour les actifs : serveurs et postes de travail) ou dans l'inventaire/catalogue d'actifs respectif (pour les actifs : solutions TI, processus, données) à côté des actifs dont ils assument la responsabilité, tel que décrit dans le registre des autorités;
> - Déterminent les règles d'accès aux actifs informationnels dont ils assument la responsabilité avec l'appui du RSI et le RAIPRP, s'il y a lieu, et assurent la mise en place d'un contrôle aléatoire des accès aux services informatiques sous leur responsabilité.

5.2.8. COMITÉ DE LA SÉCURITÉ DE L'INFORMATION (CSI)

> Ce comité (CSI) soutient les responsables dans la gestion et la coordination de la sécurité de l'information d'HÉMA-QUÉBEC.

> Il est présidé conjointement par le RSI et le RAIPRP, à titre de représentants du président et chef de la direction d'HÉMA-QUÉBEC. Il est constitué de représentants des principaux intervenants en matière de sécurité de l'information, de détenteurs d'actifs informationnels, ainsi que sur invitation, de toute personne jugée pertinente.

5.2.9. UTILISATEURS

> Les utilisateurs dûment autorisés à accéder aux actifs informationnels d'HÉMA-QUÉBEC appliquent et respectent les lois et règlements qui régissent leur domaine d'activités ainsi que la Politique globale de sécurité de l'information (PGSI), les procédures opératoires normalisées, instructions de travail, mesures et processus en matière de sécurité de l'information auxquels ils sont assujettis soit par leur lien d'emploi, par contrat ou par entente.

> Ils ont l'obligation d'informer leur gestionnaire ou le RSI de toute violation des mesures de sécurité dont ils pourraient être témoins ou de toute anomalie décelée pouvant nuire à la protection des actifs informationnels ou contrevenir à la lettre ou à l'esprit de la PGSI et des

procédures opératoires normalisées et des instructions de travail qui en découlent. Tout manquement à cette obligation sera considéré comme une faute grave, sujet aux sanctions prévues dans la PGSI.

5.2.10. GESTIONNAIRES

> Les gestionnaires sont responsables de mettre en œuvre les dispositions de la politique globale de sécurité de l'information auprès du personnel relevant de leur autorité et que :

- Les actifs informationnels mis à la disposition de leur personnel sont utilisés en conformité avec les principes généraux et les exigences de la politique globale de sécurité de l'information;
- Leurs employés sont informés de leurs obligations découlant de cette politique. Ils les informent précisément des procédures opératoires normalisées et des instructions de travail de sécurité en vigueur;
- La sécurité de l'information soit prise en compte dans tout contrat de service attribué par leur unité administrative et que tout consultant, partenaire ou fournisseur s'engage à respecter et respecte les règles de sécurité de l'information d'HÉMA-QUÉBEC;
- Tout problème d'importance en matière de sécurité de l'information soit communiqué au CSI. Ils ont l'obligation d'informer le RSI de toute violation des mesures de sécurité dont ils pourraient être témoins ou de toute anomalie décelée pouvant nuire à la protection des actifs informationnels ou contrevenir à la lettre ou à l'esprit de la PGSI et des procédures opératoires normalisées et des instructions de travail qui en découlent. Tout manquement à cette obligation sera considéré comme une faute grave, sujet aux sanctions prévues dans la PGSI.

5.2.11. RESSOURCES HUMAINES

> La direction Talent et transformation et la direction de la formation réglementaire et développement des compétences de la Vice-présidence Personnes, culture et leadership s'assurent que tout nouvel employé soit informé de ses obligations découlant de la PGSI ainsi que des procédures opératoires normalisées et des instructions de travail en vigueur en matière de sécurité de l'information et de la protection des renseignements personnels. À cet égard, elles :

- Sont responsables de la gouvernance de l'application des sanctions en cas de non-respect de la politique;
- Informent les détenteurs d'actifs des changements de statut d'un employé;
- Assurent et coordonne la formation sur la politique et s'assurent de la documentation de celle-ci au dossier de l'employé.

5.2.12. RESPONSABLE DE LA GESTION DES RISQUES ET DE LA CONTINUITÉ DES AFFAIRES

> La direction de la gestion des risques et de la continuité des affaires agit à titre de responsable de la gestion des risques et de la continuité des affaires. Ce responsable a pour rôle d'assurer la gestion et la coordination du plan de continuité des opérations (PCO). Plus particulièrement, elle :

- Coordonne l'élaboration du plan de continuité des opérations, veille à sa mise en œuvre et en assure la mise à jour;
- Assure la planification et la coordination des simulations périodiques du PCO.

5.2.13. RESPONSABLE DES INFRASTRUCTURES ET DE LA SÛRETÉ INDUSTRIELLE

> La direction des infrastructures et sûreté industrielle agit à titre de responsable de la sécurité physique. Ce responsable a pour rôle de mettre en place les mesures de protection physique des locaux et de sécurisation de leurs accès, notamment lorsqu'ils abritent des systèmes et des installations technologiques stratégiques ou essentielles ou des supports de l'information confidentielle. Plus particulièrement, le responsable de la sécurité physique :

- Conçoit et met en œuvre les mesures de protection physique des biens contre les sinistres, les pertes, les dommages, le vol ainsi que l'interruption des activités d'HÉMA-QUÉBEC;
- Élabore et met en œuvre des procédures opératoires normalisées et des instructions de travail propres à son domaine d'intervention.

5.2.14. RESPONSABLE DES AUDITS INTERNES

> La direction des audits agit à titre de responsable des audits internes. Ce responsable joue un rôle-clé dans la reddition de comptes en matière de sécurité de l'information, plus particulièrement au regard de la détermination, de l'évaluation et de la gestion des risques d'atteinte à la sécurité de l'information. À ce titre, il évalue, examine ou vérifie, notamment :

- L'application, la validité et l'efficacité des règles, des mesures administratives et des moyens technologiques en matière de sécurité de l'information élaborés et mis en œuvre;
- L'adéquation de l'intégration de la sécurité de l'information dans les processus d'affaires.

5.2.15. AFFAIRES JURIDIQUES

> La direction du secrétariat général et des affaires juridiques agit à titre de responsable de l'éthique et veille à l'intégration de l'éthique dans les processus de gestion de la sécurité de l'information, afin d'assurer la régulation des conduites et la responsabilisation individuelle.

6. Principes généraux de la politique

> HÉMA-QUÉBEC reconnaît que l'information est essentielle à ses opérations courantes et, de ce fait, qu'elle doit faire l'objet d'une évaluation, d'une utilisation appropriée et d'une protection adéquate. Entre autres, HÉMA-QUÉBEC reconnaît détenir des renseignements personnels ainsi que des informations qui ont une valeur légale, administrative ou commerciale.

> HÉMA-QUÉBEC met en place la présente politique globale de sécurité de l'information qui oriente et détermine pour l'ensemble des utilisateurs, les comportements à adopter afin de s'assurer de l'utilisation appropriée et sécuritaire de l'information et des technologies de l'information.

6.1. SANCTIONS

Lorsqu'un utilisateur contrevient ou déroge à la présente politique ou aux procédures opératoires normalisées et aux instructions de travail qui en découlent, il s'expose à des mesures disciplinaires pouvant aller jusqu'au congédiement. La gradation de la sanction est en fonction de la gravité de l'acte reproché ou de sa répétition. La mesure disciplinaire est déterminée de concert entre le supérieur de l'employé et les ressources humaines.

7. Annexe(s)

S/O

8. Liste des modifications

SECTION	DESCRIPTION DU CHANGEMENT	JUSTIFICATION	PROVENANCE DE L'INFORMATION
Toutes	Document transféré dans le nouveau gabarit de POL.	Nouveau gabarit de documents POL, disponible dans SmartSolve	SmartSolve
S/O	Suppression des numéros de PON et de leur titre, dans la section intitulée « Procédure(s) opératoire(s) normalisée(s) (PON) liée(s) ».	Les PON énumérées étaient prévues pour une entrée en vigueur en même temps que la POL-00002[0], mais n'ont pas été approuvées et ne sont jamais entrées en vigueur.	AUD-I00313, AEX-2418-EXP
1	Revue du but de la politique afin de mettre l'accent sur l'objectif de gestion des risques.	Simplification du but et emphase sur la gestion des risques.	S/O
3	Suppression de la référence au glossaire d'Héma-Québec sur L@rtère et ajout de définitions.	Le glossaire corporatif d'Héma-Québec n'est pas encore mis en place.	AUD-I00313, AEX-2418-EXP
5.2.3, 2ème flèche	Supprimé que le rôle du RAIPRP est plus amplement décrit à la DAJ-002. Ajouté une précision que le rôle du RAIPRP est sous la responsabilité de la Vice-présidence Secrétariat général, risques et audits.	Correction, le rôle du RAIPRP n'est pas décrit dans la DAJ002.	AUD-I00313, AEX-2418-EXP
5.1 schéma, 5.2 schéma, 5.2.6, 5.2.11, 5.2.12, 5.2.14, 5.2.15	Mise à jour des noms des directions et vice-présidences responsables.	Changement de la structure organisationnelle d'Héma-Québec.	Organigramme d'Héma-Québec
5.2.7,	Ajout de détails où consigner les noms des détenteurs d'actifs selon	Manquement à la POL-00002[0].	AUD-I00313, AEX-2418-EXP

SECTION	DESCRIPTION DU CHANGEMENT	JUSTIFICATION	PROVENANCE DE L'INFORMATION
1ère flèche, 3ème puce	l'inventaire d'actifs sous leur responsabilité.		
Référence : OC-07248			