

Direction générale adjointe

DE LA CYBERSÉCURITÉ
ET DE L'INFONUAGIQUE (DGACI)

CYBERSÉCURITÉ

Cadre ministériel de gestion de la
sécurité de l'information

MSSS-CDG02

2023-03-01



Table des matières

Acronymes	3
Préambule	4
Objectifs	4
Champ d'application et portée	4
Cadre légal et administratif	4
Définitions	5
Structure de gouvernance	6
Rôles et responsabilités	6
Sous-ministre	6
Chef délégué de la sécurité de l'information (CDSI)	7
Chef de la sécurité de l'information organisationnelle (CSIO)	8
Coordonnateur organisationnel des mesures de sécurité de l'information (COMSI)	10
Détenteur de l'information	11
Gestionnaire	11
Utilisateur	11
Autres intervenants dans des domaines connexes à la sécurité de l'information	12
→ Responsable de la protection des renseignements personnels (RPRP)	12
→ Responsable de l'architecture d'entreprise	12
→ Responsable de la sécurité physique	12
→ Responsable du développement sécuritaire	12
→ Responsable du plan de reprise informatique	12
→ Responsable de l'audit interne	12
→ Responsable de l'éthique	13
→ Responsable de la gestion documentaire	13
→ Responsable de l'infrastructure technologique	13
Comité sur l'accès, la protection et la sécurité de l'information (CAPSI)	13
Centre opérationnel de sécurité (COS)	13
Entrée en vigueur et révision	14

Acronymes

Acronyme	Description
CAPSI	Comité sur l'accès, la protection et la sécurité de l'information
CDSI	Chef délégué de la sécurité de l'information
CGSI	Chef gouvernemental de la sécurité de l'information
COCD	Centre opérationnel de cyberdéfense
COMSI	Coordonnateur organisationnel des mesures de sécurité de l'information
COS	Centre opérationnel de sécurité En anglais : « <i>Security operations center</i> » (SOC)
CSIO	Chef de la sécurité de l'information organisationnelle
GMVI	Gestion des menaces, des vulnérabilités et des incidents
RAG	Réseau d'alerte gouvernemental
ROCD	Responsable organisationnel de cyberdéfense
RPRP	Responsable de la protection des renseignements personnels
SI	Sécurité de l'information

Préambule

L'infonuagique, l'intelligence artificielle, la mobilité, l'Internet des objets ainsi que les nouvelles technologies de stockage et de transmission sont au cœur de l'utilisation quotidienne du numérique au ministère de la Santé et des Services sociaux (MSSS).

La stratégie de transformation numérique du MSSS permettra à terme de bonifier la prestation de services aux citoyens. Elle constitue une opportunité, mais suscite également des préoccupations majeures à considérer en lien avec la protection de l'information sensible qu'il détient, notamment celle de nature confidentielle et stratégique.

Le présent cadre de gestion s'aligne avec le cadre gouvernemental de gestion de la sécurité de l'information (SI) et complète les dispositions de la politique ministérielle de sécurité de l'information. Il fixe les rôles et les responsabilités des intervenants en SI du MSSS afin que leurs efforts contribuent efficacement à l'évolution de sa culture en la matière.

Objectifs

Le présent cadre de gestion vise à :

- instaurer une gouvernance forte et intégrée qui favorise la concertation entre les directions générales du MSSS, la complémentarité de leurs ressources et l'efficacité de leurs actions;
- définir clairement les rôles et les responsabilités des intervenants en matière de SI au MSSS;
- optimiser la concertation et la collaboration au sein de l'organisation;
- déployer une gestion optimale des événements de sécurité;
- répondre adéquatement aux exigences gouvernementales en SI.

Champ d'application et portée

Ce cadre de gestion s'applique au MSSS. Il s'applique également :

- à tous les domaines d'activités de l'organisation;
- aux ressources informationnelles et à l'information, native ou confiée au MSSS, peu importe sa nature, le support numérique sur lequel elle se trouve (enregistrement sonore ou vidéo, données électroniques ou numériques, etc.) ou sa localisation, et ce, durant tout son cycle de vie;
- à la conservation de l'information assurée par un tiers.

Cadre légal et administratif

Le cadre légal et administratif applicable est celui défini dans la politique ministérielle de sécurité de l'information et en complète les dispositions, sans toutefois s'y limiter.

Il s'inscrit notamment en conformité des exigences :

- de la Loi modifiant la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LQ 2021, chapitre 22);
- de la [Directive gouvernementale sur la sécurité de l'information](#);
- du Cadre gouvernemental de gestion de la sécurité de l'information.

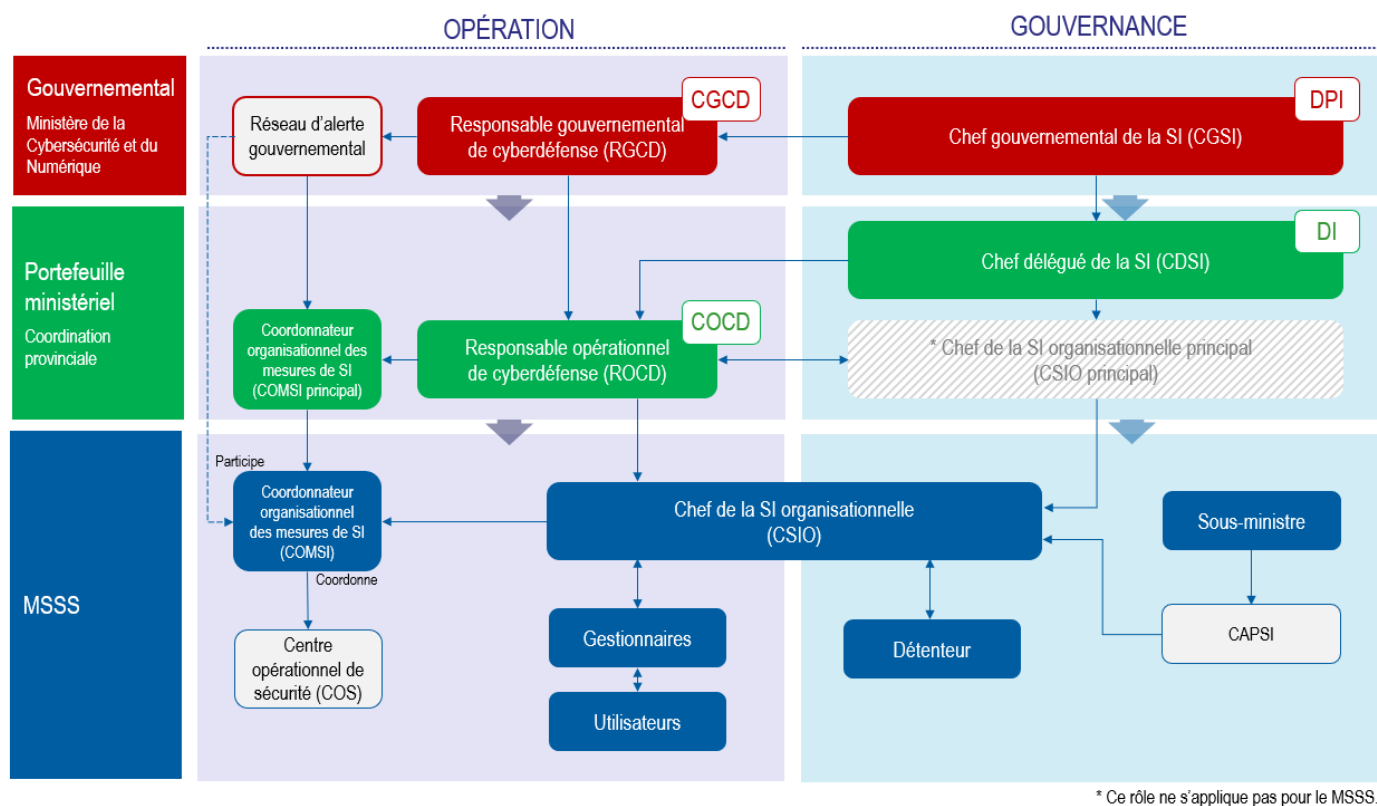
Définitions

Pour l'application du présent cadre de gestion, les termes suivants signifient :

Terme	Description
Actif informationnel	Actif au sens de la Loi sur 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 ultraspécialisé. Est également considéré comme un actif informationnel, tout support papier contenant de l'information.
Cycle de vie de l'information	L'ensemble des étapes que franchit l'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.
Détenteur de l'information	Un employé désigné par le MSSS, appartenant à la classe d'emploi de niveau-cadre ou à une classe d'emploi de niveau supérieur, et dont le rôle est, notamment, de s'assurer de la sécurité entourant de cette information ainsi que celle des ressources qui la sous-tendent, relevant de la responsabilité de son unité administrative
Événement de sécurité	Toute forme d'atteinte, présente ou appréhendée, telles une cyberattaque ou une menace à la confidentialité, à l'intégrité et à la disponibilité d'une information ou d'une ressource informationnelle sous la responsabilité d'une organisation ou d'une personne agissant pour cette dernière.
Registre d'autorité	Recueil où sont notamment consignés les noms des détenteurs de l'information, les systèmes d'information qui leur sont assignés ainsi que les noms des principaux intervenants en matière de SI.
Risque lié à la sécurité de l'information	Probabilité non nulle que survienne un événement préjudiciable à la sécurité de l'information, plus ou moins prévisible, et qui peut affecter la réalisation des objectifs d'une organisation.
Utilisateur	Toute personne de l'organisation de quelque catégorie d'emploi, de statut d'employé ainsi que toute personne morale ou physique qui, par engagement contractuel ou autrement, utilise un actif informationnel sous la responsabilité de l'organisme ou y a accès.
Système d'information	Système constitué des ressources humaines, des ressources matérielles et des procédures permettant d'acquérir, de stocker, de traiter et de diffuser les éléments d'information pertinents pour le fonctionnement d'une organisation.

Structure de gouvernance

Le MSSS adopte une structure coordonnée de gestion de la SI afin d'atteindre ses objectifs, de gérer adéquatement ses risques liés à la SI et de répondre aux exigences gouvernementales et ministérielles.



Rôles et responsabilités

La liste des responsabilités étant importante pour certains rôles, elle a été divisée par thèmes afin de favoriser une meilleure compréhension pour le lecteur.

Sous-ministre

La sous-ministre est la première responsable de la SI du MSSS. Elle est garante du respect des dispositions de la politique ministérielle de SI ainsi que de celles du présent cadre de gestion. À ce titre, elle assume les responsabilités suivantes :

- s'assurer que le MSSS soit doté d'une politique ministérielle de SI et d'un cadre ministériel de gestion de la SI, les approuver et voir à ce qu'ils soient accompagnés de mécanismes appropriés d'évaluation, de suivi et de reddition de comptes;
- s'assurer que les orientations prises en SI soient cohérentes avec la politique ministérielle, le présent cadre de gestion, les directives afférentes, les exigences gouvernementales en la matière ainsi qu'avec les besoins d'affaires du MSSS;

- s'assurer de la mise en place du Comité sur l'accès, la protection et la sécurité de l'information (CAPSI);
- assurer le maintien du lien fonctionnel entre le chef de la sécurité de l'information organisationnelle (CSIO), le chef délégué à la sécurité de l'information (CDSI) et le chef gouvernemental de la sécurité de l'information (CGSI), avec les adaptations nécessaires;
- veiller à la désignation des répondants pour les domaines spécifiques en matière de SI, lorsque le CGSI ou le CDSI le juge nécessaire.

Chef délégué de la sécurité de l'information (CDSI)

Le sous-ministre associé de la Direction générale des technologies de l'information (DGTI) détient ce rôle. À ce titre, il agit sous le lien fonctionnel du CGSI.

Le CDSI est responsable d'assurer la coordination de la SI au niveau stratégique, tactique et opérationnel pour le MSSS. À ce titre, il assume les responsabilités suivantes :

Gouvernemental

- appuyer le CGSI dans la prise en charge de l'action gouvernementale en SI;
- assurer la mise en œuvre, le respect, la coordination et le suivi des décisions et des orientations émises par le CGSI, notamment en gestion des événements de sécurité;
- agir à titre de membre invité du Comité de crise gouvernemental en sécurité de l'information (CCGSI) lorsqu'un incident touche le MSSS.

Orientations stratégiques et priorités d'action

- déterminer les orientations stratégiques et les priorités d'action pour le MSSS, dans le respect des orientations gouvernementales et des préoccupations ministérielles;
- s'assurer de mettre en œuvre tous les moyens nécessaires (ressources humaines, financières, etc.) au maintien du programme de gestion de la sécurité de l'information organisationnelle, en cohérence avec les obligations gouvernementales et la planification stratégique.

Encadrement, exigences, plans d'action

- prendre les dispositions nécessaires pour que le MSSS :
 - se dote d'une politique ministérielle de SI et d'un cadre ministériel de gestion de la SI et veille au respect des exigences qui y sont énoncées;
 - détienne un plan de reprise informatique en adéquation avec les orientations gouvernementales et ministérielles;
 - élabore un plan d'action en SI.

Organisation et opérationnalisation de la cybersécurité

- établir les attentes au CSIO pour la mise en œuvre des mesures de cybersécurité;
- désigner le responsable opérationnel de la cyberdéfense (ROCD);
- assurer la prise en charge des événements de sécurité (menaces, vulnérabilités et incidents).

Processus de gestion de la sécurité de l'information

- s'assurer de la mise en place des processus de gestion de la SI au sein du MSSS, notamment ceux portant sur la gestion de l'identité et des accès, sur le développement sécuritaire.

Événements de sécurité

- prendre toute action requise pour la prise en charge d'un événement de sécurité;
- s'assurer de l'élaboration, du maintien à jour et de l'efficacité du processus ministériel de gestion des menaces, des vulnérabilités et des incidents (GMVI);
- aviser sans délai le CGSI de tout événement de sécurité qui requiert son attention.

Gestion des risques liés à la sécurité de l'information

- s'assurer de l'élaboration et de la mise en œuvre d'un processus intégré de gestion des risques liés à la SI au MSSS.

Comités et tables

- mettre en place, coordonner et animer les comités et les groupes de travail requis à l'atteinte de la performance en matière de SI;
- représenter le MSSS à la Table gouvernementale des CDSI.

Reddition de comptes

- s'assurer de la prise en charge de toute reddition de comptes en SI requise par les instances (bilans, plans d'action, plans de redressement, etc.).

Compétences et sensibilisation

- s'assurer du développement des compétences du personnel de son ministère en SI.

Chef de la sécurité de l'information organisationnelle (CSIO)

Le directeur général adjoint du centre opérationnel de cyberdéfense (DGAC OCD) détient ce rôle. Le CSIO est désigné par le CDSI afin de le soutenir dans la coordination de la SI au niveau stratégique, tactique et opérationnel pour le MSSS. À ce titre, il assume les responsabilités suivantes :

Gouvernemental

- coordonner la mise en œuvre des processus gouvernementaux en SI au sein du MSSS;
- mettre en œuvre les décisions émanant du CGSI, du CDSI, du ROCD ainsi que du CAPSI, en coordonner l'exécution et en assurer le respect;
- assurer la coordination et la cohérence des actions en SI, conformément aux exigences gouvernementales.

Orientations stratégiques et priorités d'action

- communiquer les orientations et les priorités d'intervention gouvernementales en matière de SI aux différents intervenants du MSSS;
- assister le CDSI dans la détermination et la mise en œuvre des orientations stratégiques et des priorités d'action;

- soumettre au CAPSI les orientations, les priorités d'actions, les éléments de reddition de comptes ainsi que tout événement d'intérêt en SI.

Encadrement, exigences, plans d'action

- élaborer et faire approuver par la sous-ministre la politique ministérielle et le présent cadre de gestion au MSSS et s'assurer de leur diffusion auprès de l'ensemble du personnel du MSSS;
- veiller au respect des exigences énoncées dans la politique et le présent cadre de gestion;
- élaborer et mettre en œuvre le plan de SI et en assurer la coordination;
- assurer la cohérence des actions en SI menées par les intervenants du MSSS;
- mettre en place un cadre de développement sécuritaire qui intègre la SI, dès la phase de conception, dans les processus de développement d'actifs informationnels;
- s'assurer de l'intégration des exigences de SI lors de la réalisation de projets de développement, de l'acquisition de systèmes d'information ou d'impartition de services (ex. : infonuagique) pour le MSSS;
- s'assurer que le MSSS intègre, aux ententes de service et aux contrats sous sa responsabilité, des clauses contractuelles garantissant la SI des actifs informationnels;
- s'assurer que les détenteurs effectuent et maintiennent à jour la classification de leurs actifs informationnels et les accompagner dans cet exercice;
- s'assurer du maintien à jour du registre d'autorité du MSSS;
- s'assurer que le MSSS détienne un plan de reprise informatique en adéquation avec les orientations gouvernementales et ministérielles.

Organisation et opérationnalisation de la cybersécurité

- s'assurer que le MSSS se dote d'un Centre opérationnel de sécurité (COS)¹;
- s'assurer que le COS réalise des balayages de vulnérabilité sur les actifs informationnels du MSSS lorsque requis;
- s'assurer de la mise en place des mesures opérationnelles de SI recommandées par le ROCD ou de celles résultants des analyses des risques liés à la SI.

Processus de gestion de la sécurité de l'information

- mettre en place les processus de gestion de la SI au sein du MSSS, notamment ceux portant sur la gestion de l'identité et des accès, du développement sécuritaire, etc.

Événements de sécurité

- collaborer étroitement avec le ROCD à l'élaboration, au maintien à jour et à l'implantation du processus gouvernemental GMVI au sein du MSSS;
- mettre en œuvre les mesures de sécurité requises lors d'événements de sécurité;
- aviser sans délai le CDSI de tout événement qui requiert son attention.

¹ SOC (*Security operations center*) en anglais

Gestion des risques liés à la sécurité de l'information

- élaborer et mettre en œuvre un processus intégré de gestion des risques liés à la SI au MSSS;
- s'assurer de la contribution de l'ensemble des détenteurs et des directions générales à son évolution.

Reddition de comptes

- fournir les informations requises par le CGSI, le CDSI, le ROCD ou par toute autorité gouvernementale ou ministérielle;
- établir annuellement un bilan de SI.

Comités et tables

- coordonner et animer tout comité et groupe de travail requis pour le MSSS;
- participer activement au CAPSI.

Compétences et sensibilisation

- assurer le développement des compétences du personnel œuvrant en SI au MSSS;
- s'assurer de l'élaboration et de la mise en œuvre d'un plan de sensibilisation à la SI de l'ensemble du personnel du MSSS.

Coordonnateur organisationnel des mesures de sécurité de l'information (COMSI)

Le COMSI collabore étroitement avec le CSIO en lui fournissant le soutien technique nécessaire à l'exercice de ses responsabilités et en assurant la coordination du COS. À ce titre, il œuvre à deux niveaux :

Mesures opérationnelles de SI

- s'assurer de la mise en place effective et de l'adéquation de ces mesures au sein du MSSS, notamment celles :
 - recommandées par le ROCD (gouvernementales et ministérielles) ou par le COS;
 - résultants des analyses des risques liés à la sécurité.
- collaborer étroitement aux activités opérationnelles de SI (gestion des menaces, balayages de vulnérabilité, etc.);
- s'assurer de l'élaboration et du maintien à jour des documents portant sur la sécurité opérationnelle des actifs informationnels.

Processus GMVI

- identifier les menaces, vulnérabilités et incidents (MVI) touchant le MSSS, en tenir informé le CSIO et les escalader en fonction des conditions définies par le processus GMVI lorsque requis;
- collaborer à l'amélioration continue de ce processus, en soutien au CSIO;
- collaborer à l'élaboration, à la mise à jour et à l'application d'un plan interne de réponse aux MVI;
- participer activement au Réseau d'alerte gouvernemental (RAG).

Détenteur de l'information

Le détenteur s'assure de la protection des actifs informationnels sous sa responsabilité ainsi que du traitement approprié des risques, en collaboration étroite avec le CSIO. À ce titre, il détient la responsabilité de :

- classer les actifs informationnels sous sa responsabilité et les maintenir à jour;
- veiller à la réalisation d'analyses des risques liés à la SI pour ces actifs lors de la réalisation de projets de développement, de l'acquisition de systèmes d'information ou d'impartition de services (ex. : infonuagique) pour le MSSS ou lors de tout changement pouvant modifier l'environnement ou la configuration de l'actif;
- s'assurer de la prise en charge effective de ces risques et en approuver le niveau de risque résiduel;
- collaborer avec le CSIO, le COMSI ou avec tout intervenant en SI, à l'élaboration et à l'application des mesures de protection de ses actifs informationnels;
- aviser sans délai le CSIO de tout événement de sécurité qui requiert son attention;
- collaborer aux travaux d'audit, notamment à la mise en œuvre des recommandations qui en découlent;
- participer au processus GMVI, lorsque requis.

Gestionnaire

Le gestionnaire joue un rôle mobilisateur dans le renforcement de la culture de SI au sein de son unité administrative. À ce titre, il doit :

- informer son personnel des exigences du présent cadre et de tout document d'encadrement de la SI qui s'applique lors de l'utilisation des actifs informationnels mis à sa disposition;
- s'assurer que son personnel respecte les exigences véhiculées par le présent cadre et qu'il accède uniquement à l'information nécessaire à l'exercice de ses fonctions;
- intégrer aux ententes de services et aux contrats attribués par son unité administrative des clauses contractuelles garantissant la SI des actifs informationnels et s'assurer que tout consultant, partenaire ou fournisseur s'engage formellement à les respecter;
- communiquer rapidement au COMSI toute menace, vulnérabilité ou incident de SI dont il a connaissance, dans le respect du processus ministériel GMVI;
- veiller à ce que son personnel suive le plan de formation et de sensibilisation en SI.

Utilisateur

L'utilisateur demeure un acteur essentiel dans la protection de toute l'information mise à sa disposition dans le cadre de ses fonctions au MSSS. À ce titre, il doit :

- respecter la politique ministérielle de SI, le présent cadre de gestion, les directives afférentes ainsi que toute autre exigence gouvernementale ou ministérielle de SI;
- utiliser l'information aux seules fins auxquelles elle est destinée et dans le respect des droits qui lui sont accordés;
- respecter les droits de propriété intellectuelle lors de l'utilisation de logiciels ou de documents;
- communiquer rapidement au COMSI ou à son gestionnaire tout événement de sécurité dont il a connaissance, dans le respect du processus ministériel de GMVI.

Autres intervenants dans des domaines connexes à la sécurité de l'information

Ces intervenants ont un rôle-clé à jouer, particulièrement au regard des mesures de SI se rapportant à leurs domaines d'intervention respectifs. À ce titre, ils doivent :

- communiquer au CSIO leurs préoccupations en matière de SI;
- contribuer à la cohérence des interventions en SI lors de la mise en œuvre des processus de gestion de la SI.

Ces responsables interviennent dans les domaines suivants :

→ Responsable de la protection des renseignements personnels (RPRP)

- veiller au respect des exigences de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (PRP);
- effectuer toute recommandation en matière de PRP et ce, tout au long des projets de développement ainsi que lors de l'acquisition de systèmes d'information ou d'impartition de services (ex. : infonuagique) pour le MSSS.

→ Responsable de l'architecture d'entreprise

- s'assurer de l'intégration de la SI à la vision des technologies de l'information, en conformité avec les recommandations de l'équipe d'architecture de SI du MSSS.

→ Responsable de la sécurité physique

- appliquer les mesures de protection physique aux édifices et aux locaux en fonction des zones définies, notamment celles du Centre de traitement informatique (CTI) du MSSS;
- s'assurer de la destruction sécuritaire de tout support contenant de l'information, conformément aux exigences gouvernementales.

→ Responsable du développement sécuritaire

- intégrer la SI dans les processus de développement d'actifs informationnels dès la phase de conception, dans le respect des politiques, du présent cadre, et des directives afférentes;
- agir à titre de conseiller lors de l'acquisition de systèmes d'information pour le MSSS.

→ Responsable du plan de reprise informatique

- s'assurer que ce plan protège adéquatement les actifs informationnels du MSSS;
- s'assurer qu'il est défini, connu, testé périodiquement, mis à jour en continu et doté d'une stratégie de prise de copies quotidiennes et d'exercices de récupération périodique des données;
- veiller à l'alignement de ce plan avec le plan de continuité des services essentiels du MSSS.

→ Responsable de l'audit interne

- évaluer, examiner ou vérifier l'application, la validité et l'efficacité des règles, des mesures administratives et des moyens technologiques en SI au MSSS;
- voir à l'adéquation de l'intégration de la SI dans les processus d'affaires.

→ Responsable de l'éthique

- veiller à l'intégration de l'éthique aux processus de gestion de la SI au sein du MSSS afin d'assurer la régularisation des conduites et la responsabilisation individuelle.

→ Responsable de la gestion documentaire

- collaborer à la conception des actifs informationnels afin qu'ils détiennent les qualités nécessaires à une saine gestion de l'information, à la préservation des preuves et au respect des lois à toutes les étapes du cycle de vie de l'information (ex. : calendrier de conservation, décommissionnement des actifs, etc.).

→ Responsable de l'infrastructure technologique

- collaborer étroitement avec le COMSI dans la mise en place des correctifs de sécurité les plus récents fournis par le manufacturier ou de ceux recommandés par le COCD;
- détenir un inventaire des actifs informationnels et des composantes de l'infrastructure technologique sous sa responsabilité;
- collaborer à la mise en place et à l'évolution du plan de reprise informatique du MSSS.

Comité sur l'accès, la protection et la sécurité de l'information (CAPSI)

Le CAPSI est présidé par la sous-ministre qui peut déléguer cette responsabilité. Ce comité agit à un niveau stratégique pour la coordination et la concertation ministérielle en matière d'accès à l'information (AI), de SI et de PRP.

Le CAPSI a principalement pour rôle de :

- contribuer à définir les priorités du MSSS en matière de SI, de PRP et d'accès à l'information;
- mettre en œuvre et faire le suivi des orientations stratégiques en SI, en PRP et en AI au MSSS;
- émettre avis et recommandations sur des mandats et des orientations en lien avec tout projet ministériel comportant des enjeux en SI, en PRP ou en AI;
- valider les documents composant le cadre de gouvernance de la SI, de la PRP et de l'AI (ex. : politique, cadre de gestion, directives, plans d'action et bilans);
- traiter les enjeux de sécurité, de PRP ou de AI découlant d'un événement de sécurité (incident, menace ou vulnérabilité).

Centre opérationnel de sécurité (COS)

Le COS est sous la responsabilité du CSIO et sous la coordination du COMSI. Cette équipe a notamment pour rôle :

- réaliser les activités de détection, d'investigation, de réponse et de prévention en lien avec les cybermenaces;
- mettre en œuvre toute mesure opérationnelle requise par le gouvernement, le MSSS ou le COCD et ce, à l'intérieur des délais prescrits;
- assurer une disponibilité 24/7 pour le traitement des incidents majeurs.

Entrée en vigueur et révision

Ce cadre de gestion entre en vigueur à la date de son approbation. Il doit être révisé :

- tous les cinq ans;
- ou
- lors de changements organisationnels ou de l'adoption de nouvelles orientations gouvernementales ou ministérielles.

Approuvée par la sous-ministre du MSSS :	Dominique Savoie
Date d'approbation :	1 ^{er} mars 2023

