CADRE DE GESTION DE LA SÉCURITÉ DE L'INFORMATION

VERSION 1.0

MAI 2015

Énergie et Ressources naturelles
Québec

Historique de validation du document

Version	Date	Description des modifications
0.1	12 mars 2015	Version préliminaire pour commentaires de la ROSI
0.2	16 mars 2015	Version préliminaire intégrant les commentaires de la ROSI et des RSTI (DGARI + DGTA)
0.3	18 mars 2015	Version préliminaire intégrant les commentaires de la secrétaire générale, de la DRH et de la DRMGC
0.4	27 mars 2015	Version préliminaire intégrante les commentaires du Comité chargé de la sécurité de l'information
0.5	21 avril 2015	Révision linguistique
1.0	10 mai 2015	Document approuvé et signé par le sous-ministre

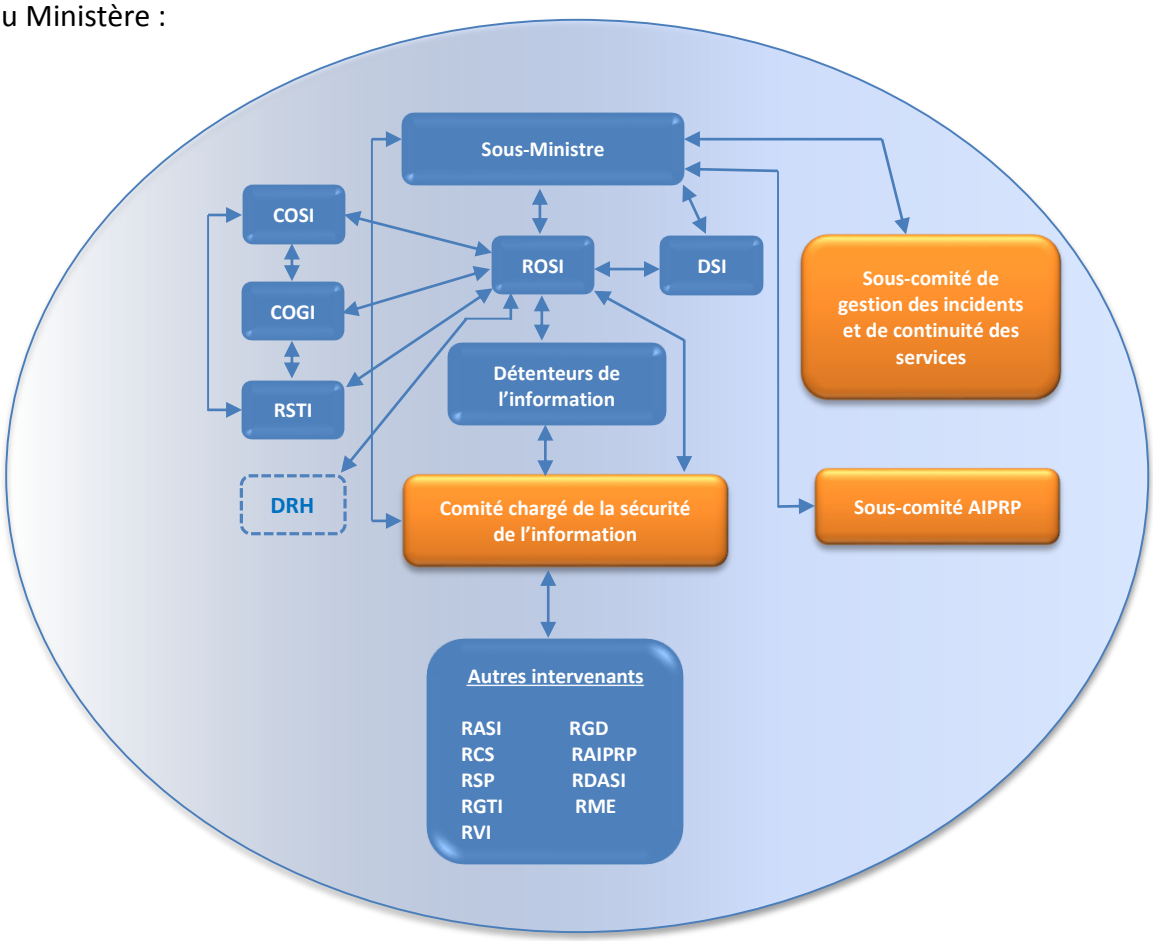
TABLE DES MATIÈRES

1. Préambule

Le Cadre de gestion de la sécurité de l'information (ci-après « Cadre de gestion ») du ministère de l'Énergie et des Ressources naturelles (ci-après « Ministère ») a pour but de compléter la Politique de sécurité de l'information en établissant la structure de gouvernance et de coordination ministérielle et en précisant les rôles et responsabilités des différents intervenants.

2. Structure de gouvernance ministérielle

Le schéma suivant illustre la structure de concertation et de coordination en sécurité de l'information au Ministère :



ROSI : Responsable organisationnel de la sécurité de l'information
DSI : Dirigeant sectoriel de l'information
COSI : Conseiller organisationnel en sécurité de l'information
COGI : Coordonnateur organisationnel de gestion des incidents
RSTI : Responsable de la sécurité des technologies de l'information
RASI : Responsable de l'architecture de sécurité de l'information
RCS : Responsable de la continuité des services
RSP : Responsable de la sécurité physique
RGTI : Responsable de la gestion des technologies de l'information
RVI : Responsable de la vérification interne
RGD : Responsable de la gestion documentaire
RAIPRP : Responsable de l'accès à l'information et de la protection des renseignements personnels
RDASI : Responsable de développement ou de l'acquisition des systèmes d'information
RME : Répondant ministériel en éthique

3. Rôles et responsabilités

La présente section décrit les rôles et responsabilités en matière de sécurité de l'information ainsi que les rôles des comités de coordination et de concertation du Ministère.

3.1. Principaux intervenants

3.1.1. Sous-ministre

En tant que premier responsable de la sécurité de l'information relevant de son autorité, le sous-ministre doit s'assurer du respect des lois et des règles de sécurité de l'information déterminées par le Secrétariat du Conseil du trésor. À ce titre, il :

- s'assure de la mise en place de mesures permettant de réduire les risques de sécurité de l'information à un niveau acceptable par l'organisation;
- s'assure de l'adéquation des mesures de sécurité de l'information en vigueur par rapport aux risques encourus;
- désigne les détenteurs de l'information, qui ont pour responsabilité de s'assurer de la sécurité de l'information relevant de l'autorité de leur unité administrative, et de la disponibilité des ressources qui la sous-tendent;
- approuve les éléments de gouvernance de la sécurité de l'information tels que la politique, le cadre de gestion, le registre d'autorité et les directives;
- préside le Comité chargé de la sécurité de l'information et les sous-comités de gestion des incidents et de l'accès à l'information et de la protection des renseignements personnels.

3.1.2. Dirigeant sectoriel de l'information (DSI)

Le DSI est désigné par le sous-ministre en vertu de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (L.R.Q. chapitre G-1.03). Il veille à l'application des règles de gouvernance et de gestion établies en vertu de la Loi sur la gouvernance et la gestion des ressources informationnelles.

À cet effet, il :

- contribue au volet informationnel des transformations organisationnelles du Ministère;

- voit à l'ensemble des activités en ressources informationnelles du Ministère, notamment en ce qui a trait au développement, à l'entretien et à l'évolution des applications ainsi qu'à l'exploitation du parc micro-informatique;

- rend compte au dirigeant principal de l'information (DPI) du Secrétariat du Conseil du trésor de l'état d'avancement de même que des résultats des projets et des autres activités en matière de ressources informationnelles;

- veille à la pérennité des actifs informationnels au sein du Ministère;

- contribue, conjointement avec le DPI et l'équipe de réponse aux incidents de sécurité de l'information de l'Administration québécoise (CERT/AQ), à la définition et à la mise en œuvre du processus de gestion des incidents à portée gouvernementale.

3.1.3. Responsable organisationnel de la sécurité de l'information (ROSI)

Le ROSI joue le rôle de porte-parole du DPI auprès du Ministère; il communique les orientations et les priorités d'intervention gouvernementales en matière de sécurité de l'information. Il assiste le sous-ministre pour ce qui est de la détermination des orientations stratégiques et des priorités d'intervention. De plus, il le représente en matière de déclaration des incidents de sécurité de l'information à portée gouvernementale. Le ROSI a, en outre, pour responsabilité :

- de soumettre à la consultation du Comité chargé de la sécurité de l'information les politiques, le cadre de gestion, les directives, les priorités d'action, les éléments de reddition de comptes ainsi que tout événement ayant mis ou qui aurait pu mettre en péril la sécurité de l'information du Ministère;

- d'assurer la coordination et la cohérence des interventions liées à la sécurité de l'information menées au sein de son organisation par d'autres intervenants dont les détenteurs de l'information, le répondant ministériel en éthique ainsi que les unités responsables des ressources informationnelles, de l'accès à l'information et de la protection des renseignements personnels, de la gestion documentaire et de la sécurité physique;

- de s'assurer de la contribution du Ministère au processus de gestion des risques et des incidents de sécurité de l'information à portée gouvernementale;

- de définir et de mettre en œuvre les processus officiels portant sur la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents ayant mis ou qui auraient pu mettre en péril la sécurité de l'information gouvernementale;

- de s'assurer de la prise en charge des exigences en matière de sécurité de l'information lors de la réalisation de projets de développement ou de l'acquisition de systèmes d'information;

- de coordonner l'élaboration et la mise en œuvre d'un programme officiel et continu de formation et de sensibilisation en matière de sécurité de l'information.

3.1.4. Conseiller organisationnel en sécurité de l'information (COSI)

Le COSI apporte son soutien au ROSI en ce qui a trait, notamment, à la mise en œuvre des mesures d'atténuation des risques et à la mise en place des processus officiels en matière de sécurité de l'information.

Au-delà de son rôle de soutien auprès du ROSI, le COSI est notamment chargé :

- de mettre en œuvre les orientations internes découlant des directives gouvernementales, des politiques internes et des bonnes pratiques en matière de sécurité de l'information;
- de produire les bilans et les plans d'action en matière de sécurité de l'information;
- d'assurer l'intégration de dispositions dans les ententes de service et les contrats garantissant le respect des exigences en matière de sécurité de l'information;
- d'assister les détenteurs de l'information dans la catégorisation de l'information relevant de leur responsabilité et la réalisation des analyses de risques de sécurité de l'information;
- d'élaborer et de tenir à jour le registre d'autorité de la sécurité de l'information;
- de contribuer à la mise en œuvre des processus officiels en matière de sécurité de l'information au Ministère.

3.1.5. Coordonnateur organisationnel de gestion des incidents (COGI)

Outre sa participation active au réseau d'alerte gouvernemental, le COGI a notamment comme responsabilité :

- de contribuer à la mise en place du processus de gestion des incidents liés à la sécurité de l'information de son organisation;
- d'assurer la coordination des membres CERT/AQ qui lui sont rattachés et de mettre en œuvre les stratégies de réaction appropriées;
- de contribuer aux analyses de risques en matière de sécurité de l'information, de déterminer les menaces et les situations de vulnérabilité et de mettre en œuvre les solutions appropriées;

- de contribuer à la mise en œuvre du processus gouvernemental de gestion des incidents liés à la sécurité de l'information;

- d'élaborer et de tenir à jour les guides portant sur la sécurité opérationnelle des systèmes et des réseaux de télécommunications;

- de collaborer étroitement avec le ROSI et de lui fournir le soutien technique nécessaire à l'exercice de ses responsabilités.

3.1.6. Responsable de la sécurité des technologies de l'information (RSTI)

En fonction de la gestion partagée des technologies de l'information (TI), le Ministère compte plus d'un RSTI. Ces derniers sont nommés par le responsable de la gestion des technologies de l'information (RGTI) de leur secteur respectif. Ils soutiennent le ROSI dans la prise en charge et la mise en œuvre de la sécurité de l'information par les différentes parties prenantes concernées. Plus précisément, un RSTI doit :

- élaborer, maintenir à jour, faire approuver et diffuser l'encadrement tactique de la sécurité des TI constitué notamment des directives et processus de gestion de la sécurité de l'information afin de soutenir la mise en œuvre de la Politique de sécurité de l'information du Ministère;

- s'assurer de la détermination des besoins et des enjeux en matière de sécurité des TI dès les premières étapes de planification stratégique pour l'ensemble des projets TI;

- coordonner la réalisation d'analyses de risques en TI, d'audits de sécurité et de tests d'intrusion;

- s'assurer de l'élaboration, de la mise en œuvre et du suivi de plans opérationnels de sécurité;

- planifier et coordonner les activités relatives aux responsabilités des autres intervenants en TI en matière de sécurité et en rendre compte sur une base régulière au ROSI;

- collaborer à la réalisation de tout dossier stratégique, tactique ou opérationnel lié aux aspects de TI de la sécurité de l'information.

3.2. Autres intervenants

3.2.1. Détenteurs de l'information

Les détenteurs de l'information désignés par le sous-ministre sont notamment chargés :

- de participer à l'élaboration des orientations stratégiques, des politiques, des cadres de gestion, des directives, des plans d'action et des bilans en matière de sécurité de l'information;

- de catégoriser l'information relevant de leur responsabilité en fonction de la disponibilité, de l'intégrité et de la confidentialité;

- de veiller à ce que les mesures de sécurité de l'information, y compris celles liées au respect des exigences légales en matière de protection des renseignements personnels, soient mises en place et appliquées;

- de s'assurer de l'adéquation des mesures de sécurité de l'information en vigueur par rapport aux risques encourus;

- d'agir comme maîtres d'œuvre des analyses de risques et de s'assurer de la prise en charge des risques résiduels pour l'information relevant de leur responsabilité.

3.2.2. Responsable de l'architecture de sécurité de l'information (RASI)

Le responsable de l'architecture de sécurité de l'information :

- conçoit et met en œuvre l'architecture décrivant la fonction, la structure et les interrelations des composantes liées à la sécurité de l'information;

- arrime les solutions retenues aux processus organisationnels en matière de sécurité de l'information;

- participe à la conception et à l'évaluation des composantes de sécurité de l'information des solutions d'affaires développées ou acquises par son organisation.

3.2.3. Responsable de la continuité des services (RCS)

Le responsable de la continuité des services assure la gestion et la coordination du plan de continuité des services de son organisation. Plus particulièrement, il :

- coordonne l'élaboration du plan de continuité des services, veille à sa mise en œuvre et en assure la mise à jour;

- assure la planification et la coordination des tests initiaux et récurrents.

3.2.4. Responsable de la sécurité physique (RSP)

Le responsable de la sécurité physique met 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 de son organisation;

- collabore à la mise au rebut sécuritaire des supports de l'information;

- élabore et met en œuvre des directives, des guides et des procédures propres à son domaine d'intervention.

3.2.5. Responsable de la gestion des technologies de l'information (RGTI)

En fonction de la gestion partagée des technologies de l'information (TI), le Ministère compte plus d'un RGTI.

Le responsable de la gestion des technologies de l'information :

- contribue à l'élaboration et à la mise en œuvre de directives contribuant à assurer la sécurité de l'information numérique;

- met en œuvre les mesures permettant d'assurer la sécurité de l'information numérique détenue par son organisation, dont les plans de reprise informatique en cas de sinistre;

- met en place un cadre normatif de développement assurant la prise en charge des exigences en matière de sécurité de l'information, y compris celles liées au respect des exigences légales de protection des renseignements personnels, lors de la réalisation d'un projet.

3.2.6. Responsable de la vérification interne (RVI)

Le responsable de la vérification interne 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'intégration de la sécurité de l'information dans les processus d'affaires.

3.2.7. Responsable de la gestion documentaire (RGD)

Le responsable de la gestion documentaire doit :

- collaborer à la conception, à l'acquisition ou au développement des systèmes informatiques, administratifs ou autres et s'assure qu'à toutes les étapes du cycle de vie de l'information ces systèmes ont les qualités nécessaires pour permettre une saine gestion des connaissances et du patrimoine informationnel, la préservation des preuves et le respect des lois;

- collaborer étroitement avec les détenteurs de l'information ainsi qu'avec le responsable ou le conseiller organisationnel en sécurité de l'information, en vue de déterminer, de gérer, de coordonner et de mettre en œuvre des mesures en matière de sécurité de l'information, indépendamment de son support;

- s'assurer de la mise en œuvre dans son organisation des politiques de gestion des documents actifs, semi-actifs et inactifs des organismes publics du gouvernement du Québec établies par Bibliothèque et Archives nationales du Québec (BAnQ);

- s'assurer de la conservation et de la gestion des documents, peu importe leur support, et ainsi :
    - établir et tenir à jour un plan de classification de manière à favoriser l'accès à l'information;
    - établir et tenir à jour un calendrier de conservation, le faire approuver par BAnQ et s'assurer de son respect;
    - élaborer, maintenir à jour et faire approuver par le sous-ministre une politique et les documents afférents sur la gestion des documents;
    - obtenir l'autorisation des gestionnaires désignés au Calendrier de conservation pour la destruction des documents dont ils sont les détenteurs principaux;
    - s'assurer de la destruction sécuritaire des documents confidentiels;
    - s'assurer du suivi des accès aux utilisateurs, autorisés par les gestionnaires des unités administratives, dans les systèmes dédiés à la gestion documentaire;
    - mettre en place un outil permettant la gestion intégrée des documents (GID).

3.2.8. Responsable de l'accès à l'information et de la protection des renseignements personnels (RAIPRP)

Le responsable de l'accès à l'information et de la protection des renseignements personnels veille au respect de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1) et du Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (chapitre A-2.1, r. 2). À ce titre, il :

- communique au responsable organisationnel de la sécurité de l'information les problèmes et les préoccupations liés à la protection des renseignements personnels ou sensibles;

- contribue à assurer la cohérence et l'harmonisation des interventions en matière de sécurité de l'information, de l'accès aux documents et de la protection des renseignements personnels, y compris lors de la mise en œuvre du processus de gestion des risques et des incidents à portée gouvernementale liés à la sécurité de l'information;

- s'assure que toute question relative aux projets d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services qui recueille, utilise, conserve, communique ou détruit des renseignements personnels soit soumise au sous-comité de l'accès à l'information et de la protection des renseignements personnels.

Au Ministère, le responsable de l'accès à l'information et de la protection des renseignements personnels exerce aussi les fonctions de ROSI.

3.2.9. Responsable du développement ou de l'acquisition de systèmes d'information (RDASI)

Le responsable du développement ou de l'acquisition de systèmes d'information conçoit, réalise et documente les fonctionnalités en matière de sécurité de l'information à intégrer aux systèmes d'information, y compris celles liées au respect des exigences légales en matière de protection des renseignements personnels. Il s'assure également de leur bon fonctionnement.

Au Ministère, le RDASI exerce aussi les fonctions de RGTI.

3.2.10. Répondant ministériel en éthique (RME)

Le répondant ministériel en éthique veille à l'intégration de l'éthique aux processus de gestion de la sécurité de l'information.

3.3. Comité chargé de la sécurité de l'information

3.3.1. Mandat

Le Comité chargé de la sécurité de l'information est la principale instance de concertation en matière de sécurité de l'information du Ministère. Plus particulièrement, il :

- examine et formule des recommandations concernant les politiques, le cadre de gestion, les directives, les plans d'action et les bilans de l'organisation, ainsi que toute proposition d'action ou état d'avancement de projets en matière de sécurité de l'information;

- analyse et formule des recommandations concernant les événements ayant mis ou qui auraient pu mettre en péril la sécurité de l'information de l'organisation.

3.3.2. Composition

Ce comité est présidé par le sous-ministre ou son représentant. Il comprend, notamment :

- la responsable organisationnelle de la sécurité de l'information (ROSI);
- le conseiller organisationnel en sécurité de l'information (COSI);
- les détenteurs de l'information;
- les responsables :
  - des ressources informationnelles;
  - de la vérification interne;
  - de l'accès à l'information et de la protection des renseignements personnels;
  - de la gestion documentaire;
  - de la sécurité physique;
  - de l'éthique.

3.3.3. Fonctionnement

- Le sous-ministre agit à titre de président du Comité chargé de la sécurité de l'information;
- Le responsable organisationnel de la sécurité de l'information (ROSI) agit comme secrétaire du Comité;
- Les détenteurs de l'information peuvent désigner un remplaçant;
- Le président du Comité chargé de la sécurité de l'information peut créer, selon les besoins, des comités *ad hoc*;
- Le Comité peut s'adjoindre toute autre personne en mesure de lui assurer le soutien adéquat dans le cadre de ses prises de décision (ex. : affaires juridiques, communication, etc.);
- Le Comité se réunit au minimum trois fois par an.

3.4. Sous-comités

Au besoin, les membres désignés pour siéger au Comité chargé de la sécurité de l'information peuvent être sollicités par le président pour participer aux sous-comités. Les sous-comités de gestion des incidents et de continuité des services sont prescrits par le Cadre gouvernemental de gestion de la sécurité de l'information du SCT alors que le sous-comité de l'accès à l'information et de la protection des renseignements personnels est prévu par le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels.

3.4.1. Sous-comité de gestion des incidents et de continuité des services

3.4.1.1. Mandat

En cas d'incident critique en matière de sécurité de l'information, le sous-comité de gestion des incidents et de continuité des services est le groupe décisionnel appelé à intervenir, notamment lorsque les tentatives de rétablissement des activités n'ont pas apporté les résultats escomptés ou qu'aucune mesure palliative n'a pu assurer la continuité ou la reprise rapide des services. À ce titre, il a pour rôle :

- d'autoriser la mise en œuvre de stratégies permettant d'assurer la prise en charge des incidents critiques liés à la sécurité de l'information;
- de procéder à l'évaluation des dommages;
- d'adopter la déclaration de sinistre proposée par le responsable de la continuité des services et d'approuver les budgets spéciaux correspondants;
- de décider du déploiement ou non du plan de continuité des services et d'en assurer la mise en œuvre, le cas échéant;
- de proposer des orientations à suivre ou des actions à poser en cas de sinistre;
- de formuler des recommandations concernant le délestage de certaines des activités de l'organisation;
- d'assurer la coordination avec les intervenants de l'extérieur de l'organisme public, le cas échéant.

3.4.1.2. Composition

Ce sous-comité est présidé par le sous-ministre ou son représentant et le noyau permanent est composé :

- des représentants de la haute direction;
- du responsable organisationnel de la sécurité de l'information (ROSI);
- du conseiller organisationnel en sécurité de l'information (COSI);
- du coordonnateur organisationnel de gestion des incidents (COGI);
- du responsable de l'accès à l'information et de la protection des renseignements personnels (RAIPRP);
- du responsable de la sécurité physique (RSP);
- du responsable de la continuité des services (RCS).

Ce sous-comité peut s'adjoindre toute autre personne en mesure de lui assurer le soutien adéquat dans le cadre de ses prises de décision (exemple : les détenteurs de l'information ou les conseillers pour les volets juridique, technologique et de communication avec les médias et les ressources humaines).

3.4.2. Sous-comité de l'accès à l'information et de la protection des renseignements personnels

3.4.2.1. Mandat

Le sous-comité est chargé de soutenir le sous-ministre dans l'exercice de ses responsabilités et obligations en matière d'accès à l'information et de protection des renseignements personnels. Il doit, notamment :

- veiller à l'application du Règlement sur la diffusion de l'information et sur la protection des renseignements personnels au sein du Ministère;
- analyser toute question relative aux projets d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services qui recueille, utilise, conserve, communique ou détruit des renseignements personnels;
- s'assurer que les mesures particulières en matière de protection des renseignements personnels relatives au sondage ou à une technologie de vidéosurveillance sont respectées.

3.4.2.2. Composition

Ce sous-comité est présidé par le sous-ministre ou son représentant et est composé :

- du responsable de l'accès à l'information et à la protection des renseignements personnels (RAIPRP);
- du responsable organisationnel de la sécurité de l'information (ROSI);
- du responsable de la gestion documentaire (RGD);
- du répondant ministériel en éthique (RME).

4. Dispositions finales

4.1. Mise en œuvre, suivi et révision

Le responsable organisationnel de la sécurité de l'information (ROSI), appuyé par le conseiller organisationnel en sécurité de l'information (COSI), est responsable de l'élaboration et de l'application du Cadre de gestion.

Celui-ci sera révisé à l'occasion des changements importants qui pourraient l'affecter ou, au plus tard, tous les trois ans à partir de la date d'approbation. Toute modification devra être approuvée par le sous-ministre sur recommandation du Comité chargé de la sécurité de l'information.

4.2. Approbation et date d'entrée en vigueur

Ce cadre de gestion remplace le Cadre de gestion de la sécurité de l'information approuvée le 4 mars 2009. Il entre en vigueur à la date d'approbation.

Original signé 10 mai 2015

_____ _____

M. Gilbert Charland Date

Sous-ministre