

Cadre de gestion de la sécurité de l'information

Version 1.1

31 mars 2009

Historique des modifications

Version	Date de création/ mise à jour	Auteur	Description des modifications
0.1	9 juin 2008	Benoit Lessard	<ul style="list-style-type: none"> ▪ Version préliminaire pour commentaires du dir. BSMS et des membres du Bureau de l'accès à l'information et de la protection des renseignements personnels (BAIPRP)
0.2	24 juillet 2008	Benoit Lessard	<ul style="list-style-type: none"> ▪ Version intégrant les commentaires du dir. BSMS et des membres du BAIPRP ▪ Version <u>préliminaire</u> pour commentaires de la DGTI, de la DRM et d'intervenants de Foncier Québec
0.2.1	31 octobre 2008	Benoit Lessard	<ul style="list-style-type: none"> ▪ Version intégrant la première série de commentaires de la DGTI, de la DRM et d'intervenants de Foncier Québec ▪ Version en prévision de la seconde série de commentaires de la DGTI, de la DRM et d'intervenants de Foncier Québec ainsi qu'auprès de directions ciblées
0.3	8 décembre 2008	Benoit Lessard	<ul style="list-style-type: none"> ▪ Version intégrant la seconde série de commentaires de la DGTI, de la DRM, d'intervenants de Foncier Québec et de directions ciblées ▪ Version pour commentaires des SMA et du DG resp. de Faune Québec et ceux des membres du CMSAI ainsi que pour une révision linguistique
0.4	15 janvier 2009	Benoit Lessard	<ul style="list-style-type: none"> ▪ Version intégrant les commentaires des SMA et du DG resp. de Faune Québec et ceux des membres du CMSAI ainsi que les corrections linguistiques retenues ▪ Version pour recommandation d'approbation par les membres du CMSAI
0.5	5 février 2009	Benoit Lessard	<ul style="list-style-type: none"> ▪ Version pour adoption par les membres du CD-MRNF
0.5.1	23 février 2009	Benoit Lessard	<ul style="list-style-type: none"> ▪ Version ajustée pour tenir compte des changements apportés à la structure administrative du SCSP qui entreront en vigueur le 2 mars 2009 ▪ Version pour adoption par les membres du CD-MRNF
1.0	3 mars 2009	Benoit Lessard	<ul style="list-style-type: none"> ▪ Document approuvé, signé par le sous-ministre
1.1	31 mars 2009	Benoit Lessard	<ul style="list-style-type: none"> ▪ Version amendée pour tenir compte du message du sous-ministre du 26 mars 2009 concernant la nomination d'un sous-ministre associée à Faune Québec et de la mise à jour de l'organigramme du Ministère

La rédaction de ce cadre de gestion a été inspirée notamment par :

- le cadre légal et normatif en vigueur;
- les différents guides produits par le gouvernement du Québec;
- la documentation reçue des ministères et organismes suivants : la Régie de l'assurance maladie du Québec, Services Québec, la Commission administrative des régimes de retraite et d'assurances et le ministère des Finances du Québec.

NOTE : Dans le présent document, le générique masculin est utilisé sans aucune discrimination et uniquement dans le but d'alléger le texte.

Bureau de la sécurité de l'information
 Direction du Bureau du sous-ministre et du Secrétariat
 Ministère des Ressources naturelles et de la Faune
 5700, 4e Avenue Ouest, bureau A 303
 Québec (Québec) G1H 6R1

© Gouvernement du Québec

Table des matières

1.	INTRODUCTION	1
2.	OBJECTIFS	1
3.	RAPPEL - EXTRAIT DE LA POLITIQUE	2
3.1.	DÉFINITION DE LA SÉCURITÉ DE L'INFORMATION (SI).....	2
3.2.	OBJECTIFS DE LA SI	2
4.	STRUCTURE DE GOUVERNANCE	3
4.1.	ORGANISATION GOUVERNEMENTALE DE LA SÉCURITÉ DE L'INFORMATION	3
4.2.	ORGANISATION MINISTÉRIELLE DE LA SÉCURITÉ DE L'INFORMATION	4
4.3.	REDDITION DE COMPTE.....	5
4.4.	STRUCTURE DE CONCERTATION ET DE COORDINATION	6
4.4.1.	Comité de direction (CD-MRNF)	6
4.4.2.	Comité ministériel de sécurité et d'accès à l'information (CMSAI).....	6
4.4.2.1.	Sous-comités.....	6
5.	RÔLES ET RESPONSABILITÉS	7
5.1.	PROMOTEURS DE LA SI	7
5.1.1.	Sous-ministre	7
5.1.2.	Responsable de la sécurité de l'information (RSI).....	8
5.1.3.	Mandataires d'éléments de l'actif informationnel.....	8
5.2.	RESPONSABLES CONCERNÉS PAR LA MISE EN ŒUVRE DE LA SI	9
5.2.1.	Sous-ministres associés.....	9
5.2.2.	Représentants sectoriels de la SI et des mandataires de ce secteur	10
5.2.3.	Directeur de la Direction des ressources matérielles (DRM).....	10
5.2.4.	Responsables de la gestion des TI (RGTI) au SCSP et à Foncier Québec	11
5.2.5.	Gestionnaires.....	12
5.2.5.1.	Gestion de projet.....	12
5.2.6.	Utilisateurs	12
5.2.7.	Direction de l'évaluation et de la vérification (DEV)	13
5.2.7.1.	DEV, volet Enquêtes	13
5.2.8.	Direction générale des affaires stratégiques et du territoire (DGAST)	14
5.2.9.	Direction des ressources humaines (DRH)	14
5.3.	RESPONSABLES DES SPÉCIALITÉS CONCERNÉES PAR LA SI.....	14
5.3.1.	Responsable de l'accès à l'information et de la protection des renseignements personnels (RAIPRP).....	15
5.3.2.	Responsable de la gestion documentaire (RGD).....	16
5.3.3.	Responsable de la sécurité des personnes et des biens (RSPB)	16
5.3.4.	Répondant en éthique.....	17
5.3.5.	Responsables de la sécurité des TI (RSTI).....	17
5.3.6.	Agents de liaison technique (ALT)	18
6.	DISPOSITIONS FINALES	19
6.1.	MISE EN ŒUVRE, SUIVI ET RÉVISION	19
6.2.	APPROBATION ET DATE D'ENTRÉE EN VIGUEUR	19
	ANNEXE 1 – GLOSSAIRE	21
	ANNEXE 2 – LISTE DES MEMBRES DU CMSAI	25
	ANNEXE 3 – LES SOUS-COMITÉS DU CMSAI	27

Liste des acronymes

ALT	Agent de liaison technique
BAnQ	Bibliothèque et Archives nationales du Québec
CD-MRNF	Comité de direction du ministère des Ressources naturelles et de la Faune
CERT/AQ	Équipe de gestion des incidents cybernétiques du gouvernement du Québec
CGSI	Cadre de gestion de la sécurité de l'information
CISP	Centre interministériel de services partagés
CMSAI	Comité ministériel de sécurité et d'accès à l'information
COSSIG	Comité d'orientation stratégique de la sécurité de l'information gouvernementale
CSPQ	Centre de services partagés du Québec
DEV	Direction de l'évaluation et de la vérification
DGAST	Direction générale des affaires stratégiques et du territoire
DRH	Direction des ressources humaines
DRM	Direction des ressources matérielles
GID	Gestion intégrée des documents
MRNF	Ministère des Ressources naturelles et de la Faune
MSG	Ministère des Services gouvernementaux
PGSI	Plan global de la sécurité de l'information
PRP	Protection des renseignements personnels
RAIPRP	Responsable de l'accès à l'information et de la protection des renseignements personnels
RGD	Responsable de la gestion documentaire
RGTI	Responsable de la gestion des technologies de l'information
RSI	Responsable de la sécurité de l'information
RSPB	Responsable de la sécurité des personnes et des biens
RSTI	Responsable de la sécurité des technologies de l'information
SCSP	Secteur de la Coordination et des Services partagés
SI	Sécurité de l'information
TI	Technologies de l'information

1. Introduction

Découlant de la *Politique concernant la sécurité de l'information* (Politique), le *Cadre de gestion de la sécurité de l'information* (Cadre de gestion) établit la structure de gouvernance et de coordination ministérielle en sécurité de l'information (SI). Il énonce formellement les rôles et responsabilités pour soutenir la mise en œuvre et la prise de décision en vue de l'atteinte des objectifs de la SI¹.

Le Cadre de gestion sert de fondement pour la mise en place de processus formels de gestion intégrée et en continu de la SI ainsi que des risques afférents. Il formalise, pour le ministère des Ressources naturelles et de la Faune (MRNF), un modèle évolutif correspondant à des façons de faire reconnues et généralement utilisées à l'échelle provinciale, nationale et internationale.

De plus, il ne faut pas ignorer l'influence sur la SI que peuvent avoir les facteurs de changements de diverses natures qu'ils soient : technologique, organisationnel, juridique ou sociétal. Ces changements, en raison de leurs impacts possibles sur la qualité de la SI, sont à considérer lors de la révision et de la mise à jour tant de la Politique que du Cadre de gestion.

Enfin, la mise en œuvre de la SI au sein du MRNF fera l'objet de plans d'action. Ces différents plans de sécurité, sous la forme de plans de mise en œuvre sectorielle et de plans opérationnels de sécurité, seront synthétisés dans un plan global de la SI. Ce dernier permettra d'effectuer un suivi ministériel des activités des plans d'action.

2. Objectifs

Le Cadre de gestion vise principalement à :

- établir une structure de gouvernance et de coordination ministérielle;
- énoncer formellement un ensemble de rôles et de responsabilités en SI.

¹ Les objectifs de la SI sont établis à la section 1.2 de la Politique et repris à la section 3.2 du présent document.

3. Rappel - Extrait de la Politique

3.1. Définition de la sécurité de l'information (SI)

La sécurité de l'information (SI), c'est l'ensemble des activités qui préservent la disponibilité, l'intégrité et la confidentialité de l'information, et ce, peu importe le support utilisé pour la conserver ou la transmettre. C'est aussi un ensemble de mesures de sécurité pour assurer l'authentification des personnes et des dispositifs ainsi que de l'irrévocabilité des actions qu'ils posent.

Cette définition implique que la SI s'applique à tous les aspects de la sûreté, de la garantie et de la protection d'une information, quel que soit son support. En bref, la SI concerne : les différentes infrastructures; les domaines que sont l'accès à l'information, la protection des renseignements personnels et la gestion documentaire; la problématique de la continuité des services et celle de la protection des personnes et des biens; et les façons d'être, l'éthique.

3.2. Objectifs de la SI

La SI doit permettre de maintenir et même, de rehausser la confiance des citoyens à l'égard de l'État et des services publics qu'il rend et de contribuer à la réalisation de la mission de l'État et à celle du MRNF.

En tenant compte des risques et de leurs impacts pour le Ministère et le gouvernement, les mesures de sécurité à maintenir ou à mettre en place doivent être proportionnelles à la valeur de l'information à protéger. Elles visent à :

- **assurer la disponibilité** de l'information de façon à ce qu'elle soit accessible en temps voulu et de la manière requise par une personne autorisée;
- **assurer l'intégrité** de l'information de manière à ce qu'elle ne soit pas détruite ou altérée de quelque façon, sans autorisation, et que le support de cette information lui procure la stabilité et la pérennité voulues;
- **assurer la confidentialité** de l'information en limitant sa divulgation aux seules personnes autorisées à en prendre connaissance, assurant ainsi une stricte confidentialité;
- permettre de confirmer l'identité d'une personne ou l'identification d'un document ou d'un dispositif;
- se prémunir contre le refus d'une personne de reconnaître sa responsabilité à l'égard d'un document ou d'un autre objet, dont un dispositif d'identification avec lequel elle est en lien.

4. Structure de gouvernance

Le Cadre de gestion établit la structure de gouvernance du MRNF en présentant dans quel contexte celle-ci s'insère. L'organisation de la SI, tant gouvernementale que ministérielle, permet d'établir une vision commune et intégrée de la SI en vue d'assurer la cohérence, la coordination et l'intégration des préoccupations des intervenants en la matière, et ce, aussi bien aux plans stratégique, tactique qu'opérationnel.

4.1. Organisation gouvernementale de la sécurité de l'information

Tel qu'illustré dans le schéma présenté à la page suivante, l'ensemble des parties prenantes de l'organisation gouvernementale de la SI mettent au centre de leurs préoccupations la protection de l'information gouvernementale. Ainsi, les ministères et organismes ont la responsabilité de protéger cette information et, lorsque nécessaire, de la rendre disponible aux citoyens et entreprises.

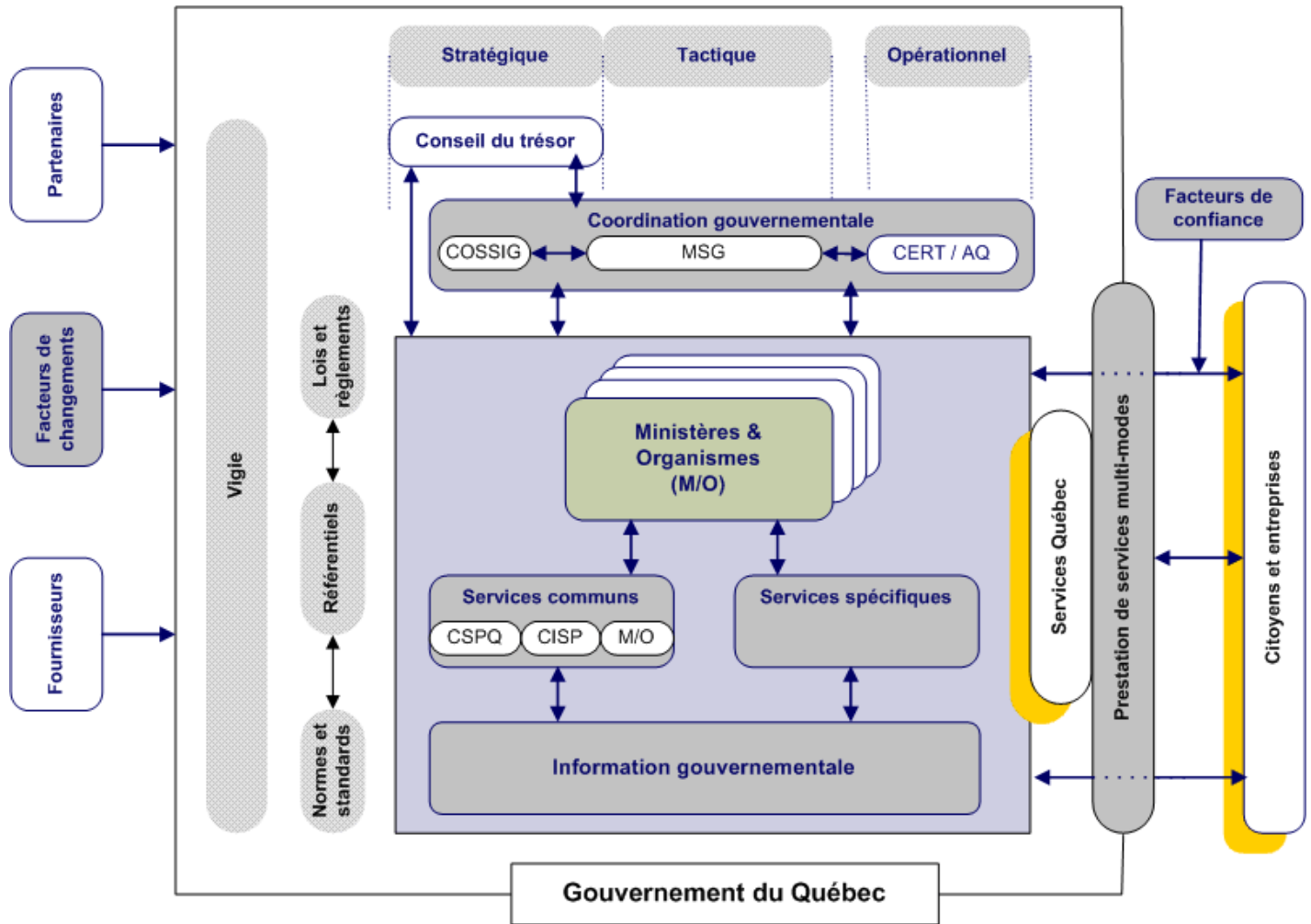
Au sein de l'organisation gouvernementale, le Conseil du trésor exerce son rôle de gouverne au point de vue stratégique. Le ministère des Services gouvernementaux (MSG) s'active également aux plans stratégique et tactique en proposant au Conseil du trésor les objectifs et les contrôles stratégiques en SI. Il assure la coordination de la SI à l'échelle gouvernementale et celle du Comité d'orientation stratégique de la sécurité de l'information gouvernementale (COSSIG) et apporte le soutien nécessaire aux ministères et organismes. Au plan opérationnel, l'Équipe de gestion des incidents cybernétiques du gouvernement du Québec (CERT/AQ) assure la coordination des incidents cybernétiques à l'échelle gouvernementale et soutient les ministères et organismes en cette matière.

Enfin, parmi les ministères et organismes responsables d'infrastructures technologiques ou de services communs avec qui le MRNF entretient un partenariat, on retrouve :

- Services Québec, dont la mission est d'offrir aux citoyens et aux entreprises, sur tout le territoire du Québec, un guichet unique multiservice afin de leur permettre un accès simplifié à des services publics;
- le Centre de services partagés du Québec (CSPQ) dont la mission est de fournir ou de rendre accessibles les biens et les services administratifs dont les organismes publics ont besoin dans l'exercice de leurs fonctions, notamment en matière de ressources humaines, financières, matérielles et informationnelles et de moyens de communication;
- ceux ayant le statut de Centre interministériel de services partagés (CISP), tel que Revenu Québec qui offre des services d'enquêtes administratives.

Le schéma I illustre aussi les principaux éléments de renforcement de la SI gouvernementale que sont : la vigie, les normes et les standards, les référentiels, les lois et règlements ainsi que les facteurs de confiance.

Schéma I - Organisation gouvernementale de la sécurité de l'information²



4.2. Organisation ministérielle de la sécurité de l'information

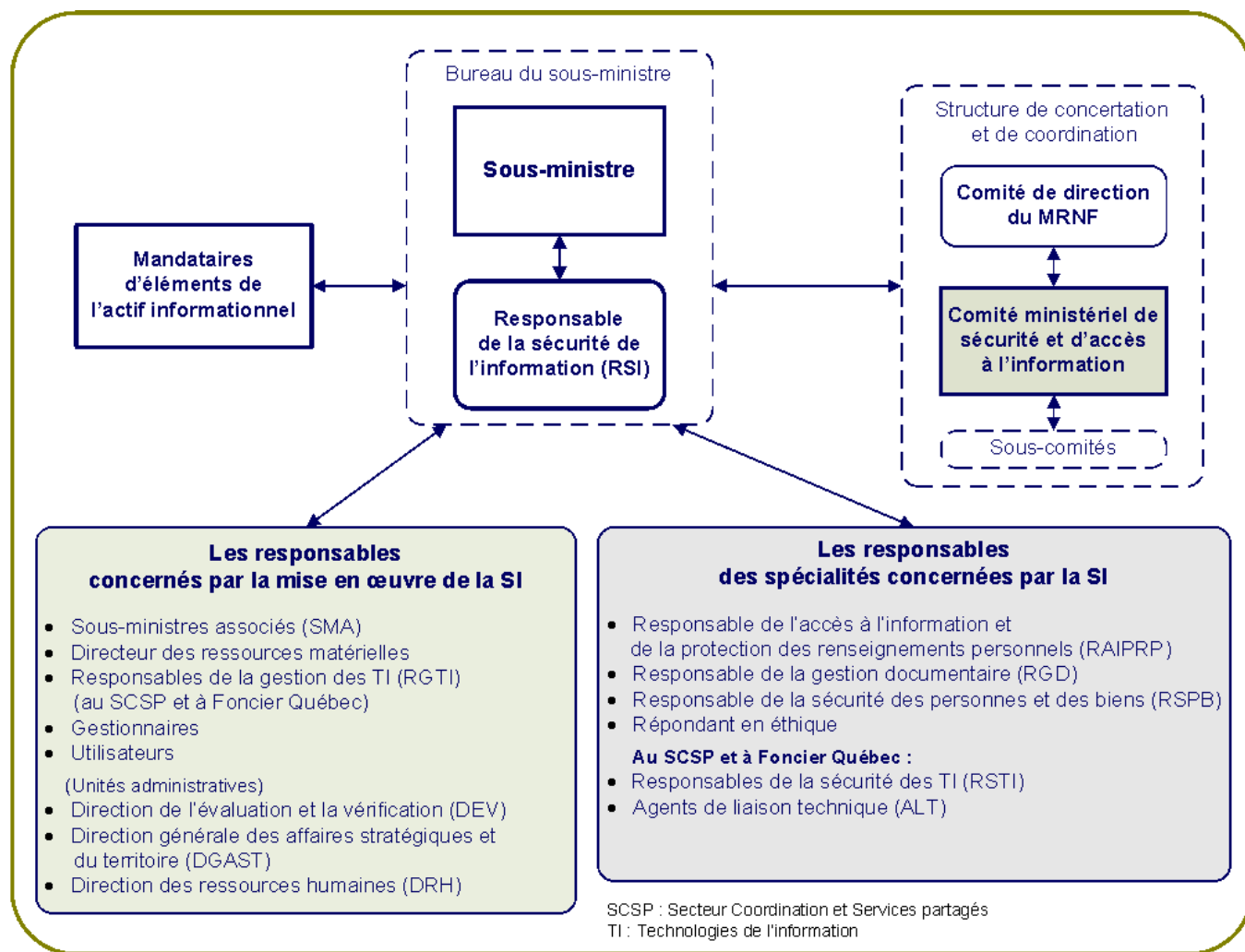
Enchâssée dans l'organisation gouvernementale et représentée par le schéma II, l'organisation ministérielle de la sécurité de l'information du MRNF :

- établit la structure de concertation et de coordination;
- énonce les principaux rôles pour soutenir la prise de décision et la mise en œuvre des mesures de sécurité nécessaires pour atteindre les objectifs de la SI.

Chacun des éléments présentés au schéma II est expliqué dans les sections subséquentes.

² Schéma extrait du *Modèle de gestion de la sécurité de l'information gouvernementale*, Gouvernement du Québec, 4 juillet 2007, page 24.

Schéma II - Organisation ministérielle de la sécurité de l'information du MRNF



4.3. Reddition de compte

Rendre compte, c'est répondre de ce que l'on a fait ou de ce qui s'est produit et justifier les résultats obtenus. Une personne nommée pour assumer un rôle répond de l'exercice des responsabilités associées à ce rôle. En SI, on rend compte :

- de manière formelle, par la voie hiérarchique, auprès des responsables concernés par la mise en œuvre de la SI et, éventuellement, auprès du sous-ministre;
- de manière informelle, par la voie fonctionnelle, auprès du RSI et des responsables des spécialités concernées.

La forme que peut prendre la reddition de compte est variable. L'une des formes privilégiées est le plan de sécurité, soit : le plan global de la SI pour le Ministère, un plan de mis en œuvre pour un secteur et, par spécialités concernées par la SI, un plan opérationnel de sécurité.

En tenant compte des ressources disponibles, les plans de sécurité comportent un ensemble d'objectifs à atteindre en vue d'atténuer les risques et de mettre en œuvre la Politique, le Cadre de gestion et les autres éléments du Cadre administratif de la SI. Cette mise en œuvre doit aussi se concrétiser dans une perspective d'amélioration continue dans l'intention d'améliorer sans cesse la qualité de ce qui est réalisé.

4.4. Structure de concertation et de coordination

4.4.1. Comité de direction (CD-MRNF)

Les membres du CD-MRNF soutiennent et conseillent le sous-ministre, notamment dans ses responsabilités en matière de SI. À ce titre, ils commentent et recommandent l'approbation ou le refus des dossiers qui leur sont présentés.

4.4.2. Comité ministériel de sécurité et d'accès à l'information (CMSAI)

Présidé par le sous-ministre ou son représentant, le CMSAI assume un rôle stratégique en matière de sécurité de l'information, d'accès à l'information et de protection des renseignements personnels. Le CMSAI a trois mandats :

- soutenir le sous-ministre dans l'exercice de ses responsabilités et obligations;
- assurer la coordination, la concertation, la cohérence et l'intégration des préoccupations et des interventions stratégiques en SI;
- répondre aux obligations énoncées par la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q., c. A-2.1) et sa réglementation.

Plus particulièrement, le CMSAI doit notamment :

- soutenir la mise en œuvre des orientations stratégiques;
- proposer et recommander des priorités d'intervention et les budgets à y associer;
- favoriser la cohérence des actions en SI;
- commenter, recommander et assurer le suivi des éléments de gouvernance de la SI dont le *Plan global de la sécurité de l'information* (PGSI);
- être informé des incidents de sécurité, des rapports de vérification concernant la SI et des travaux des comités ad hoc en SI.

4.4.2.1. Sous-comités

Pour s'acquitter de ses responsabilités, le CMSAI peut confier la réalisation de travaux à des sous-comités (voir l'annexe 3).

5. Rôles et responsabilités

5.1. Promoteurs de la SI

5.1.1. Sous-ministre

Le sous-ministre est le premier responsable de la SI. À ce titre, il s'assure du respect des lois et des directives présentées à l'annexe 1 de la Politique, ainsi que les règles de sécurité déterminées par le Conseil du trésor.

Il doit en outre :

- nommer un responsable de la sécurité de l'information (RSI), un répondant en éthique, un mandataire pour chacun des éléments de l'actif informationnel et leur déléguer les pouvoirs associés à leurs responsabilités;
- définir clairement les valeurs organisationnelles et les orientations internes, les faire partager par l'ensemble du personnel et s'assurer qu'elles sont respectées en les communiquant aux partenaires et aux fournisseurs du Ministère;
- établir un processus formel de gestion intégrée et d'amélioration continue de la SI et, à cette fin, définir une structure organisationnelle de SI où les rôles et les responsabilités en cette matière sont clairement attribués à des personnes identifiées à tous les niveaux de l'organisation;
- instaurer un mécanisme d'identification et d'évaluation périodique des risques en matière de SI ainsi que de l'adéquation des mesures de sécurité en vigueur par rapport à ces derniers;
- lorsque demandé ou prévu par une convention, présenter aux instances gouvernementales ou aux partenaires d'affaires les plans de sécurité, les bilans ou autres conformément aux instructions convenues avec ceux-ci.

Plus spécifiquement, il doit :

- approuver les éléments de gouvernance de la sécurité de l'information, tel que : la politique, le cadre de gestion, le registre d'autorité et les directives;
- accepter les risques résiduels à la suite d'une analyse de risques et approuver les plans de sécurité;
- lorsque requis, être informé des incidents de sécurité;
- présider le Comité ministériel de sécurité et d'accès à l'information (CMSAI) ou nommer un représentant pour assumer cette responsabilité.

5.1.2. Responsable de la sécurité de l'information (RSI)

Nommé par le sous-ministre afin de le représenter en matière de gestion et de coordination de la SI dans l'organisation, le RSI assiste ce dernier dans la détermination des orientations stratégiques et des priorités d'intervention. En plus de soutenir et d'accompagner les différents intervenants du MRNF, le RSI peut intervenir sur tout sujet ou activité concernant la SI.

Le RSI doit :

- élaborer, maintenir à jour et faire approuver par le sous-ministre les éléments de gouvernance de la SI tels que la politique, le cadre de gestion et le registre d'autorité;
- élaborer, maintenir à jour et faire approuver par le sous-ministre certains éléments³ qui découlent de la gouvernance de la SI, soit celles ayant une portée ministérielle et concernant plus d'une spécialité de la SI;
- s'assurer de la réalisation d'analyses de risques en SI ainsi que de l'élaboration et de l'approbation de plans de sécurité et de leur suivi;
- s'assurer que les intervenants prennent en compte dans leurs responsabilités les orientations stratégiques en SI⁴;
- lorsque requis, être informé des incidents de sécurité;
- élaborer, mettre en œuvre et tenir à jour un programme de gestion de la continuité incluant la réalisation d'exercices;
- s'assurer de la formation et de la sensibilisation des utilisateurs;
- mettre en place une stratégie de veille concernant la SI;
- être informé des rapports de vérification concernant la SI;
- siéger au CMSAI et aux comités auxquels il est convié;
- lorsque requis en matière de SI, siéger à des comités interministériels, représenter l'organisation et faire le lien avec les entités gouvernementales;
- rendre compte de ses travaux au sous-ministre et au CMSAI.

5.1.3. Mandataires d'éléments de l'actif informationnel

À titre de premier responsable de la sécurité de l'information et de détenteur des éléments de l'actif informationnel du MRNF, le sous-ministre nomme des cadres pour assumer les responsabilités de mandataire pour un ou plusieurs éléments de l'actif informationnel du Ministère. Ces nominations sont consignées au *Registre d'autorité de la sécurité de l'information*.

³ Un de ces éléments sera l'*Architecture ministérielle de sécurité de l'information* (AMSI), et ce, après l'entrée en vigueur de l'*Architecture gouvernementale de sécurité de l'information* (AGSI).

⁴ Les orientations stratégiques en SI sont établies à la section 5. Énoncés de sécurité de la Politique.

Avec le soutien des différents intervenants en SI, un mandataire est tenu de s'assurer que les mesures de sécurité appropriées sont élaborées, approuvées, mises en place et appliquées systématiquement aux éléments de l'actif informationnel sous sa responsabilité. Il doit notamment :

- établir, prescrire et réviser les règles pour l'attribution des privilèges d'accès aux éléments de l'actif informationnel sous sa responsabilité, s'assurer périodiquement de leur respect et autoriser toute exception;
- répondre de l'utilisation faite par les utilisateurs autorisés pour les éléments de l'actif informationnel sous sa responsabilité;
- comprendre la nature et la portée des éléments de l'actif informationnel sous sa responsabilité ainsi que leurs liens avec les processus d'affaires et les autres éléments afin notamment d'en déterminer leurs valeurs de catégorisation;
- participer au processus d'analyse et de gestion des risques concernant les éléments de l'actif informationnel sous sa responsabilité;
- s'assurer que les exigences de sécurité et les mesures de sécurité appropriées pour atténuer les risques ou atteindre les objectifs de sécurité sont élaborées, mises en place et appliquées systématiquement aux éléments de l'actif informationnel sous sa responsabilité;
- être informé des incidents de sécurité ou des vulnérabilités affectant les éléments de l'actif informationnel sous sa responsabilité;
- s'assurer de l'élaboration et du maintien à jour de la documentation concernant chacun des éléments de l'actif informationnel sous sa responsabilité;
- rendre compte de la gestion des éléments de l'actif informationnel sous sa responsabilité au sous-ministre associé concerné et, lorsque requis en matière de SI, en tenir informé le représentant sectoriel de la SI et le RSI.

5.2. Responsables concernés par la mise en œuvre de la SI

5.2.1. Sous-ministres associés

Les sous-ministres associés s'assurent de la prise en compte de la SI dans leurs activités sectorielles et énoncent leurs besoins et leurs intentions en la matière.

Chacun d'eux doit :

- s'assurer de la mise en œuvre de la SI dans son secteur;
- soutenir dans leurs responsabilités les mandataires des éléments de l'actif informationnel du secteur;
- désigner un représentant sectoriel à titre de membre du CMSAI;
- commenter les éléments de gouvernance de la SI;
- lorsque requis, être informé des incidents de sécurité;
- rendre compte au sous-ministre de la mise en œuvre de la SI dans son secteur.

5.2.2. Représentants sectoriels de la SI et des mandataires de ce secteur

Nommé par un sous-ministre associé, le représentant sectoriel de la SI et des mandataires de ce secteur assiste ce dernier dans ses responsabilités et le représente au sein du secteur et du CMSAI.

Avec le soutien des différents intervenants en SI, et ce, en conformité avec la *Politique concernant la sécurité de l'information* et les documents afférents, le représentant sectoriel de la SI doit notamment :

- s'assurer de la réalisation d'analyses de risques en SI, de l'élaboration et de l'approbation de plans de sécurité et en assurer les suivis;
- être informé des rapports de vérification concernant la SI;
- être informé des rapports d'évaluation de programme et des recommandations concernant la SI;
- siéger au CMSAI et aux comités auxquels il est convié;
- rendre compte de ses travaux au sous-ministre associé ainsi qu'au CMSAI et en tenir informé le RSI.

5.2.3. Directeur de la Direction des ressources matérielles (DRM)

La DRM offre une multitude de produits et de services qu'elle a regroupés par grands domaines d'activités dont l'approvisionnement en biens et services, la gestion des lieux de travail, la gestion immobilière, la gestion des systèmes de télécommunications voix/image et la gestion de la connaissance. La sécurité des personnes et des biens ainsi que la gestion documentaire sont aussi sous l'encadrement du directeur de la DRM.

En plus d'être le mandataire de l'immobilier utilisé par le MRNF, ce directeur doit :

- nommer et soutenir un responsable de la sécurité de personnes et des biens (RSPB) et un responsable de la gestion documentaire (RGD);
- en matière de SI, accompagner les gestionnaires dans la planification et l'évaluation de leurs besoins d'affaires;
- conseiller et soutenir les mandataires dans la mise en place des mesures de sécurité appropriées pour chacun des éléments de l'actif informationnel sous leur responsabilité;
- s'assurer de la réalisation d'analyses de risques, de l'élaboration et de l'approbation de plans opérationnels de sécurité ainsi que de leurs suivis;
- mettre en œuvre les solutions nécessaires pour atteindre les objectifs fixés et réaliser les mesures prévues aux différents plans de sécurité;
- lorsque requis, être informé des incidents de sécurité;
- s'assurer que les préoccupations de SI sont intégrées au processus de gestion des conventions;
- rendre compte de la gestion de la sécurité des personnes et des biens et de la gestion documentaire au sous-ministre associé concerné et au CMSAI ainsi qu'en tenir informé le représentant sectoriel de la SI et le RSI.

5.2.4. Responsables de la gestion des TI (RGTI) au SCSP et à Foncier Québec

La gestion des technologies de l'information (TI) du Ministère est assumée par deux secteurs et formalisée par une entente⁵. Les services de TI sous la gouverne du SCSP sont offerts à tous les secteurs du Ministère, à l'exception de Foncier Québec, qui n'utilise que certains de ces services. Ceux sous la gouverne de Foncier Québec sont offerts seulement pour ce Secteur.

En plus d'être mandataire de l'infrastructure technologique sous leur gouverne, les responsables de la gestion des TI assument les mêmes responsabilités en matière de SI avec une étendue différente. Un responsable de la gestion des TI doit :

- nommer et soutenir un responsable de la sécurité des TI (RSTI) et un agent de liaison technique (ALT);
- en matière de SI, accompagner les gestionnaires dans la planification et l'évaluation de leurs besoins d'affaires;
- conseiller et soutenir les mandataires dans la mise en place des mesures de sécurité appropriées pour chacun des éléments de l'actif informationnel sous leur responsabilité;
- s'assurer de la réalisation d'analyses de risques, de l'élaboration et de l'approbation de plans opérationnels de sécurité ainsi que de leurs suivis;
- mettre en œuvre les solutions nécessaires pour atteindre les objectifs fixés et réaliser les mesures prévues aux différents plans de sécurité;
- lorsque requis, être informé des incidents de sécurité;
- siéger au CMSAI et aux comités auxquels il est convié;
- rendre compte de la gestion de la sécurité des TI au sous-ministre associé concerné et au CMSAI ainsi qu'en tenir informé le représentant sectoriel de la SI et le RSI.

En s'inspirant des normes et bonnes pratiques et en conformité avec la *Politique concernant la sécurité de l'information* et les documents afférents, il doit formellement :

- organiser, encadrer et maintenir à jour les rôles et les responsabilités aux plans tactique et opérationnel en sécurité des TI;
- établir et tenir à jour une structure de coordination de sécurité des TI;
- inclure la SI dans l'offre de services en TI et dans les ententes de services;
- s'assurer que la gestion des risques et la SI sont prises en compte dès le début des projets en TI;
- s'assurer de l'élaboration, du maintien à jour et de la mise en œuvre d'un cadre normatif qui tient compte des exigences⁶ de la sécurité, du contrôle et de la protection des renseignements personnels.

⁵ Entente de collaboration entre le Secteur de la Coordination et des Services partagés et Foncier Québec en matière de technologies de l'information, mai 2008.

⁶ Ces exigences sont inscrites dans l'outil méthodologique *Précis Sécurité, contrôle et protection des renseignements personnels* (Précis SCPRP), développé pour le MSG par DMR Conseil.

5.2.5. Gestionnaires

Avec le soutien des différents intervenants en SI, un gestionnaire doit s'assurer de la mise en œuvre de la SI au sein de son unité administrative et du respect, par les utilisateurs sous son autorité (personnel et consultants), des règles émises. Un gestionnaire (un cadre) doit notamment :

- assumer, *de facto*, les responsabilités de mandataire pour les éléments de l'actif informationnel de son unité administrative qui ne sont pas répertoriés au *Registre d'autorité de la sécurité de l'information*;
- formuler les demandes ou les retraits de privilèges d'accès à l'information pour les utilisateurs de son unité administrative;
- réviser périodiquement les privilèges d'accès à l'information octroyés aux utilisateurs de son unité administrative et s'assurer qu'ils n'ont accès qu'à l'information nécessaire à l'exercice de leurs fonctions;
- informer son soutien technique habituel, le mandataire d'éléments de l'actif informationnel ou le RSI de tout problème, incident, menace ou vulnérabilité pouvant affecter la SI;
- soutenir le programme ministériel de sensibilisation en matière de SI;
- mettre en œuvre, lorsque nécessaire, les mesures administratives, disciplinaires ou légales concernant les utilisateurs sous sa responsabilité;
- rendre compte de la mise en œuvre de la SI au sein de son unité administrative et du respect des règles à son gestionnaire hiérarchique et, selon l'importance du sujet, en tenir informé le représentant sectoriel de la SI ou le RSI.

5.2.5.1. Gestion de projet

En plus de respecter et de mettre en œuvre les exigences spécifiques pour la gestion et le contrôle de son projet, incluant les budgets ainsi que l'évaluation des coûts de réurrences, un gestionnaire de projet (aussi appelé chef de projet) a des responsabilités importantes de gestion de la SI. Un gestionnaire de projet doit :

- prendre en compte la SI dans toutes les phases du projet;
- respecter les cadres légaux, administratifs et normatifs en vigueur;
- identifier les nouveaux risques introduits par le projet et en informer le mandant du projet (aussi appelé directeur de projet) et, selon l'importance du risque, le RSI;
- lorsque requis, présenter le projet au Sous-comité sur la protection des renseignements personnels (voir l'annexe 3) et mettre en œuvre les mesures recommandées.

5.2.6. Utilisateurs

Les responsabilités les plus importantes, assumées par l'ensemble des utilisateurs, sont de respecter et de mettre en pratique les règles émises en SI. Pour ce faire, un utilisateur doit notamment :

- prendre connaissance et respecter la *Politique concernant la sécurité de l'information* ainsi que tous les documents afférents;

- protéger l'information mise à sa disposition, l'utiliser avec discernement et aux seules fins prévues;
- utiliser les éléments de l'actif informationnel conformément aux lois, aux directives, aux politiques et aux exigences en matière de sécurité, et ce, de manière éthique, à l'intérieur des accès qui lui sont autorisés;
- assumer la responsabilité des actions qu'il pose concernant son utilisation des éléments de l'actif informationnel du Ministère;
- participer aux activités de sensibilisation et de formation en matière de SI;
- lorsque requis, participer et contribuer à la réalisation d'un projet;
- signaler à son gestionnaire ou au soutien technique habituel, tout problème, incident, menace ou vulnérabilité qu'il perçoit.

5.2.7. Direction de l'évaluation et de la vérification (DEV)

En continuité avec son mandat, la DEV s'assure de la conformité et de l'efficacité des contrôles en vue de l'application de la *Politique concernant la sécurité de l'information* et des documents afférents.

À cette fin, elle doit notamment :

- effectuer des vérifications indépendantes et objectives des activités en SI et en faire rapport au sous-ministre;
- fournir, sur demande, des avis et des conseils quant à la sécurité des éléments de l'actif informationnel;
- effectuer des vérifications concernant la conformité des conventions auprès des fournisseurs et des partenaires du Ministère à l'égard de leurs obligations en matière de SI;
- faire le lien avec le Vérificateur général du Québec;
- rendre compte de ses travaux au sous-ministre et en tenir informé le CMSAI.

5.2.7.1. DEV, volet Enquêtes

En plus, la DEV assume un rôle opérationnel de coordination ou de réalisation d'enquêtes. À ce titre, elle doit notamment :

- établir et maintenir à jour un protocole d'intervention pour encadrer la collecte, l'utilisation, la conservation, la transmission et la destruction de preuves;
- communiquer aux responsables de la gestion des TI et aux mandataires ses besoins en matière de journalisation et d'outils d'exploitation;
- lorsque requis, être informée des incidents de sécurité;
- après l'approbation du sous-ministre, transmettre le résultat d'une enquête à tout corps de police compétent ou au Procureur général du Québec;
- rendre compte de ses travaux au sous-ministre et, lorsque requis, en informer le RSI.

5.2.8. Direction générale des affaires stratégiques et du territoire (DGAST)

Un des mandats de la DGAST est de concevoir, de mettre à jour et d'assurer le suivi annuel d'un plan ministériel de gestion des risques stratégiques. En matière de SI, la DGAST doit principalement :

- établir les exigences, les balises et les métriques ministérielles afin d'uniformiser l'identification et l'évaluation des risques en SI;
- conseiller le RSI lors de l'identification et de l'évaluation des risques en SI;
- tenir compte des risques de SI dans un plan annuel de gestion des risques.

5.2.9. Direction des ressources humaines (DRH)

La DRH a pour mandat de s'assurer que le Ministère dispose de la main-d'œuvre requise en proposant à la direction ainsi qu'au personnel des orientations et des services permettant de créer un environnement de travail qui favorise la mobilisation, le développement et la santé au travail, dans le respect des conditions de travail qui régissent le personnel. Ainsi, dans le cadre de l'application de la *Politique concernant la sécurité de l'information*, la DRH doit notamment :

- exercer un rôle conseil auprès du gestionnaire en matière d'imposition de mesures administratives et disciplinaires pour des manquements relatifs à la Politique;
- analyser, valider et, le cas échéant, acheminer à la DEV⁷ toute requête spécifique d'un gestionnaire souhaitant que soit réalisée une vérification ou une enquête à l'égard d'un membre de son personnel.

5.3. Responsables des spécialités concernées par la SI

Les responsables des spécialités concernées par la SI coordonnent les activités ayant une incidence tactique ou opérationnelle. En tenant compte des orientations⁸ stratégiques en SI et des plans de sécurité, ils s'assurent que les mesures de sécurité appropriées pour atténuer les risques ou atteindre les objectifs de la SI sont élaborés, mises en place et appliquées. Ils s'assurent aussi du suivi des interventions spécifiques à leur spécialité qui découlent de la gouvernance de la SI.

Les responsables des spécialités concernées par la SI sont :

- le responsable de l'accès à l'information et de la protection des renseignements personnels (RAIPRP);
- le responsable de la gestion documentaire (RGD);
- le responsable de la sécurité des personnes et des biens (RSPB);
- le répondant en éthique;

⁷ Se référer à la section 5.2.7.1 DEV, volet Enquêtes du présent document

⁸ Les orientations stratégiques en SI sont établies à la section 5. Énoncés de sécurité de la Politique.

et, concernant les technologies de l'information, des responsables distincts pour le SCSP de ceux de Foncier Québec :

- les responsables de la sécurité des TI (RSTI);
- les agents de liaison technique (ALT).

Pour ce faire, un responsable d'une des spécialités doit :

- élaborer, planifier, coordonner et réaliser la planification annuelle ou pluriannuelle des activités liées à sa spécialité ainsi que les activités de communication, de sensibilisation et de formation spécifiques à sa spécialité;
- collaborer à la réalisation des travaux auxquels il est convié;
- être informé des rapports de vérification concernant sa spécialité;
- siéger aux comités auxquels il est convié;
- lorsque requis pour sa spécialité, siéger aux comités interministériels, représenter l'organisation et faire le lien avec les entités gouvernementales;
- tenir informé le RSI de ces travaux.

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

Délégué⁹ par le ministre et soutenu par le Bureau de l'accès à l'information et de la protection des renseignements personnels, le RAIPRP doit répondre aux obligations de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q., c. A-2.1) et sa réglementation ainsi que s'assurer de son application au MRNF.

En plus des responsabilités regroupées à la section 5.3 du Cadre de gestion, le RAIPRP doit notamment :

- s'assurer de l'élaboration, de la mise à jour et de l'approbation des mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support;
- être informé des incidents de sécurité liés à sa spécialité et les documenter;
- établir et maintenir un réseau de répondants en accès à l'information (AI), protection des renseignements personnels (PRP) et, par extension, en SI;
- siéger au CMSAI;
- rendre compte de ses travaux au sous-ministre et au CMSAI.

⁹ Article 8 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q., c. A-2.1)

5.3.2. Responsable de la gestion documentaire (RGD)

Nommé par le directeur de la DRM, le RGD doit s'assurer de la mise en œuvre 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). Il doit aussi s'assurer de la conservation et de la gestion des documents, peu importe leur support.

En plus des responsabilités regroupées à la section 5.3 du Cadre de gestion, le RGD doit notamment :

- établir et tenir à jour un plan de classification de manière à favoriser l'accès à l'information¹⁰;
- établir et tenir à jour un calendrier de conservation, le faire approuver par la BAnQ¹¹ et s'assurer de son observation;
- élaborer, maintenir à jour et faire approuver par le sous-ministre une politique et les documents afférents concernant la gestion des documents;
- siéger au CMSAI;
- rendre compte de ses travaux au directeur de la DRM et au CMSAI.

Lors de l'entrée en vigueur des exigences gouvernementales à établir par la BAnQ pour la conservation et la gestion intégrée des documents (GID), le RGD devra :

- élaborer et faire approuver par le sous-ministre les exigences ministérielles pour la conservation et la GID;
- proposer au sous-ministre et mettre en place un outil permettant la GID afin de mettre en oeuvre ces exigences.

5.3.3. Responsable de la sécurité des personnes et des biens (RSPB)

Nommé par le directeur de la DRM, le RSPB coordonne la mise en oeuvre de mesures visant à assurer la sécurité des personnes et des biens dans les lieux utilisés par le Ministère. De façon générale, il soutient, par ses interventions spécialisées, l'atténuation des risques ou l'atteinte des objectifs de sécurité. Il peut intervenir sur tout sujet ou activité concernant sa spécialité.

En plus des responsabilités regroupées à la section 5.3 du Cadre de gestion, le RSPB doit notamment :

- élaborer et tenir à jour les données relatives aux menaces et aux risques encourus par le Ministère au regard des locaux qu'il occupe et des clients qu'il dessert;
- mettre en place des mesures visant la gestion des accès aux lieux utilisés par le Ministère ainsi que le contrôle de la circulation des biens sortant de ces lieux;

¹⁰ En conformité avec l'article 16 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q., c. A-2.1)

¹¹ En conformité avec la *Loi sur les archives* (L.R.Q., chapitre A-21.1)

- s'assurer de l'identification des besoins liés à la sécurité des personnes et des biens ainsi qu'à la gestion des accès dès les premières étapes de planification des différents projets d'aménagement des locaux au MRNF;
- s'assurer de l'élaboration et de l'évolution de divers plans (mesures d'urgence ou autres) ainsi que de la réalisation d'exercices;
- être informé et assurer de la prise en charge des incidents de sécurité liés à sa spécialité et les documenter;
- élaborer, maintenir à jour, faire approuver et diffuser la réglementation encadrant sa spécialité;
- rendre compte de ses travaux au directeur de la DRM.

5.3.4. Répondant en éthique

Nommé par le sous-ministre, le répondant en éthique se doit d'établir et de maintenir un processus de réflexion continu sur le sens et les conséquences multiples des actions qui permet de soutenir la prise de décision, d'assurer la régulation des conduites et la responsabilisation individuelle.

En plus des responsabilités regroupées à la section 5.3 du Cadre de gestion, le répondant en éthique doit notamment :

- Coordonner, en matière de SI, la démarche éthique visant à assurer la responsabilisation individuelle et la régularisation de la conduite des utilisateurs;
- rendre compte de ses travaux au sous-ministre.

5.3.5. Responsables de la sécurité des TI (RSTI)

Pour tenir compte de la gestion partagée des TI, le MRNF compte plus d'un RSTI qui assument les mêmes responsabilités en matière de sécurité des TI avec des étendues différentes. Nommé par un responsable de la gestion des TI, le RSTI l'assiste dans la mise en œuvre de ces responsabilités et dans la détermination des priorités d'intervention.

Au plan tactique, le RSTI s'assure que la sécurité des TI est mise en œuvre au sein de son secteur et par sa clientèle. Il prend en charge la coordination des activités en sécurité des TI et s'assure de leur réalisation. Lorsqu'il le requiert, le RSTI intervient sur tout sujet ou activité concernant sa spécialité selon son étendue.

En plus des responsabilités regroupées à la section 5.3 du Cadre de gestion, le RSTI doit notamment :

- élaborer, maintenir à jour, faire approuver et diffuser l'encadrement tactique de la sécurité des TI;
- s'assurer de l'identification des besoins et enjeux de sécurité des TI dès les premières étapes de planification stratégique pour l'ensemble des projets TI;
- s'assurer de la réalisation d'analyses de risques, de l'élaboration et de l'approbation de plans opérationnels de sécurité et en assurer le suivi;
- être informé des incidents de sécurité liés à sa spécialité et les documenter;

- s'assurer de l'élaboration et de l'évolution de divers plans (secours, reprise informatique ou autres) ainsi que de la réalisation d'exercices;
- établir et maintenir une interrelation avec les autres RSTI, les ALT, le RSPB et le RSI;
- rendre compte de ses travaux à son responsable de la gestion des TI.

5.3.6. Agents de liaison technique (ALT)

Le gouvernement du Québec s'est doté, en 2002, d'un centre spécialisé dans la coordination et la gestion des incidents informatiques à l'échelle gouvernementale, le CERT/AQ. En cas d'incident informatique, celui-ci apporte aux ministères et organismes un soutien personnalisé en matière de prévention, de détection et de réaction. De plus, le CERT/AQ assure la coordination d'un réseau d'alertes gouvernemental qui implique la participation active des ALT des ministères et organismes.

Pour tenir compte de la gestion partagée des TI, le Ministère est représenté par deux ALT au sein de ce réseau. Ils assument les mêmes responsabilités en matière de sécurité des TI avec une étendue différente. Ce rôle opérationnel est spécifique à la prévention et à la réaction aux incidents liés à la sécurité des TI. Il collabore étroitement avec différents intervenants, dont l'ALT de l'autre secteur, les RSTI, le RSPB et le RSI.

En plus des responsabilités regroupées à la section 5.3 du Cadre de gestion, l'ALT doit notamment :

- établir et maintenir un réseau d'ALT interne¹² ainsi qu'un réseau de contacts externes, principalement avec le CERT/AQ et les ALT des autres ministères et organismes;
- être informé et assurer de la prise en charge des incidents de sécurité des TI, informer les intervenants appropriés et coordonner une équipe de réponse aux incidents de sécurité des TI;
- élaborer et maintenir à jour les pratiques de sécurité opérationnelle;
- contribuer aux analyses des risques, identifier les menaces et les vulnérabilités et proposer des solutions appropriées;
- participer à l'élaboration et à l'évolution de divers plans (secours, reprise informatique ou autres) ainsi qu'à la réalisation d'exercices;
- rendre compte de ses travaux à son responsable de la gestion des TI et au RSTI.

¹² Les ALT internes sont des intervenants identifiés comme étant des spécialistes TI ou des administrateurs des systèmes et des réseaux.

6. Dispositions finales

Le présent document remplace le *Registre d'autorité de la sécurité de l'information numérique*, DSI, MRNFP, Janvier 2003.

6.1. Mise en œuvre, suivi et révision

La coordination de la mise en œuvre du Cadre de gestion ainsi que la mise à jour de ce document relève du responsable de la sécurité de l'information du MRNF.

Afin d'assurer son adéquation aux besoins en sécurité de l'information au Ministère, le présent Cadre de gestion doit être révisé annuellement après son entrée en vigueur ou lors de changements significatifs qui pourraient l'affecter.

6.2. Approbation et date d'entrée en vigueur

Le présent *Cadre de gestion de la sécurité de l'information* est approuvé et entre en vigueur à la date de la signature par le sous-ministre. Néanmoins, les annexes du Cadre de gestion peuvent être mises à jours après leurs adoptions par le CMSAI.

Original signé

2009-03-04

Normand Bergeron
Sous-ministre du MRNF

Date

Annexe 1 – Glossaire

Les définitions inscrites dans ce glossaire sont majoritairement extraites du *Grand dictionnaire terminologique* de l'Office québécois de la langue française ou en sont inspirées.

Actif informationnel

Inventaire présentant, à un moment déterminé, le portrait de l'ensemble des ressources informationnelles d'une organisation, à l'exception des ressources humaines.

L'actif informationnel est un bilan et ne donne que le portrait des ressources informationnelles disponibles; il est de ce fait statique. Ce sont les ressources informationnelles qui sont dynamiques puisque ce sont elles qu'on exploite.

L'actif informationnel peut inclure une banque d'information électronique, un système d'information, un processus d'affaires, une technologie de l'information ou une installation, ou encore un ensemble de ces éléments acquis ou constitués par une organisation. La notion d'« *actif* » fait référence à un ensemble. Lorsqu'on veut désigner un élément de l'actif, on doit utiliser l'appellation restrictive « *élément d'actif informationnel* ».

Catégorisation

Processus d'assignation d'une valeur à certaines caractéristiques d'une information, lesquelles caractérisent le degré de sensibilité de cette information et, conséquemment, la protection à lui accorder.

Continuité des activités

Processus hiérarchisé qui vise à atténuer les impacts en cas d'incident majeur ou de sinistre affectant la disponibilité de l'information, et ainsi permettre le rétablissement des activités ou processus d'affaires essentiels et stratégiques dans un délai acceptable de façon planifiée et préparée.

Document

Un ensemble constitué d'information portée par un 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 transcriposables sous l'une de ses formes ou en un autre système de symboles. Est assimilée au document toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite.

Évaluation de programme

L'évaluation de programme est une démarche rigoureuse de collecte et d'analyse d'information qui vise à porter un jugement sur un programme, une politique, un processus ou un projet pour aider à la prise de décision concernant les orientations à privilégier dans l'avenir. Elle peut permettre d'apprécier à la fois la pertinence du programme, l'efficacité avec laquelle ses objectifs sont poursuivis, l'efficience des moyens d'exécution ou la rentabilité ainsi que l'impact du programme.

Fournisseur

Un organisme public ou une personne physique ou morale qui fait affaire avec le Ministère en vue de lui fournir des services ou des biens.

Gestion de projet

Mode de réalisation d'un projet où l'application des techniques de gestion pendant le cycle de vie du projet permet d'atteindre des objectifs précis. Les techniques de gestion sont un ensemble d'activités nécessaires à la planification, à la coordination et au contrôle du déroulement de l'exécution d'un projet.

Dès les premières étapes de planification d'un projet, les enjeux et besoins en SI doivent être identifiés et énoncés ainsi que ceux des bénéficiaires du projet. Cette façon de procéder doit permettre principalement :

- d'intégrer à la planification d'un projet ces enjeux et besoins;
- d'améliorer la précision des évaluations financières des projets, et ce, en incluant les activités qui concernent la SI;
- de mettre en œuvre ou d'ajuster les services de SI offerts en prévision de nouveaux projets.

Incident de sécurité

Circonstance au cours de laquelle la disponibilité, l'intégrité ou la confidentialité d'un ou plusieurs éléments de l'actif informationnel du Ministère ont été affectées. De même que toute situation présentant les conditions requises pour potentiellement produire un tel résultat.

Un incident de sécurité peut être le fruit d'un désastre naturel, d'un bris matériel, d'une erreur humaine ou d'un acte malveillant. Sont considérés comme actes malveillants : la fraude, l'indiscrétion, le détournement d'information ainsi que le sabotage immatériel, tel que le sabotage manuel et les attaques cybernétiques (incluant les attaques de dénis de service, les intrusions, l'envoi de pourriel, les vers et virus et autres).

Mandataire d'éléments de l'actif informationnel

Gestionnaire désigné comme responsable d'un ou plusieurs éléments de l'actif informationnel nécessaire à la conduite des activités d'une organisation.

Mesure de sécurité

Moyen organisationnel, technologique, humain ou juridique permettant d'assurer la réalisation des objectifs de disponibilité, d'intégrité et de confidentialité de l'information ainsi que d'authentification des personnes et des dispositifs et de l'irrévocabilité des actions qu'ils posent.

Partenaire

Organisation avec laquelle une autre organisation collabore pour atteindre des objectifs convenus en commun.

Personnel

Ensemble des personnes employées par le Ministère de quelque catégorie d'emploi ou de statut, incluant les gestionnaires.

Plans de sécurité

Inspiré de la méthode MÉHARI¹³, il y a trois types de plans de sécurité, soit :

- le plan stratégique de la sécurité de l'information (PSSI) :
Le PSSI concerne la vision globale, la recherche de cohérence et les orientations à long terme de l'organisation. La rédaction d'un plan stratégique de la sécurité de l'information répond à deux impératifs d'une bonne gestion des risques :
 - définir une stratégie de sécurité dont les objectifs sont conformes aux enjeux de l'organisme;
 - garantir la cohérence des actions en matière de sécurité au sein de chaque unité administrative de l'organisme.
- les plans opérationnels de la sécurité (POS)
(ou plan de mise en œuvre sectorielle) :
Les POS sont élaborés pour chacune des unités administratives concernées et particulièrement celles étant responsables d'une spécialité de la SI. Les choix de solutions précises adaptées aux différents contextes observés, aux méthodes de travail et aux technologies seront concrétisés dans ces plans de sécurité. Les POS sont souvent déduits directement du diagnostic de l'analyse des risques au moment de l'évaluation des mesures en place.
Un plan de mise en œuvre sectorielle est établi de manière similaire à un POS à l'échelle d'un secteur ou encore, une consolidation des différents plans de sécurité d'un secteur.
- le plan global de la sécurité de l'information (PGSI) :
Le PGSI est la version consolidée de tous les POS des unités administratives. Il peut être vu comme la synthèse des POS. Cette consolidation permet, entre autres, d'identifier les impacts des mesures choisies sur les activités de toutes les unités administratives touchées par la mesure. De plus, il permet un suivi des activités des plans d'action du point de vue global de l'organisation.

Privilège d'accès

Privilège accordé à une personne ou à une entité d'avoir accès à de l'information, des documents, des programmes déterminés et de les exploiter d'une façon particulière ou encore des lieux. Si l'accès est physique, il ne peut être accordé qu'à des personnes. L'accès logique, lui, peut concerner tout aussi bien des personnes que d'autres entités, comme un système informatique.

Privilège d'accès élevés

Privilège particulier réservé à une autorité, c'est-à-dire à personne ou à une entité exerçant des responsabilités importantes relativement à la protection et à la gestion des systèmes d'information ou d'un lieu stratégique. Les privilèges d'accès élevés font l'objet de mesures de sécurité particulière.

Processus d'affaires

Suite cohérente d'activités et d'opérations commerciales qu'une organisation entretient avec des tiers, traduisant les besoins de ses clients et les exigences de son environnement, et tenant compte ou non de ses activités internes, de manière à les agencer selon une logique de création de valeur.

¹³ Méthode Harmonisée de Risques Informatiques, CLUSIF (www.clusif.asso.fr)

Programme de gestion de la continuité

Processus de gestion holistique identifiant les impacts potentiels menaçant une organisation et qui fournit une structure pour développer la résilience avec la capacité de reprise qui protège principalement les intérêts des parties prenantes, la réputation ainsi que les opérations.

Promoteur

Personne qui donne la première impulsion à un projet, à un mouvement, qui en provoque la création et qui, éventuellement, en assure la réalisation.

Registre d'autorité

Recueil où sont inscrites les désignations des personnes affectées à des responsabilités particulières concernant la gestion de la sécurité de l'information.

Sécurité des technologies de l'information (Sécurité des TI)

Ensemble des mesures de sauvegarde visant à préserver la confidentialité, l'intégrité, la disponibilité, l'utilisation prévue et la valeur des renseignements conservés, traités ou transmis par voie électronique. Le terme *sécurité des TI* inclut aussi les mesures de protection appliquées aux biens utilisés pour recueillir, traiter, recevoir, afficher, transmettre, reconfigurer, balayer, entreposer ou détruire l'information par voie électronique.

Sécurité des personnes et des biens (SPB)

Aspect de la sécurité qui traite des mesures physiques prises pour assurer la protection des personnes et des biens. Les mesures visent notamment à empêcher l'accès physique non autorisé aux équipements, installations et documents ainsi que les protéger contre toute forme de menaces ou de risques.

Sociétal

Qui se rapporte à la société en tant que communauté d'êtres humains, à ses valeurs et à ses institutions

Utilisateurs

Toutes personnes (physiques ou morales) ayant accès, sur place ou à distance, à l'information, aux biens ou aux lieux pour lesquels le MRNF a la responsabilité d'assurer la sécurité. Un utilisateur se définit comme étant :

- le personnel du MRNF (les employés incluant les gestionnaires);
- les partenaires gouvernementaux ou d'affaires;
- les fournisseurs;
- les clients du MRNF.

Annexe 2 – Liste des membres du CMSAI

Le Comité ministériel de sécurité et d'accès à l'information (CMSAI) est constitué de membres et de conseillers. Le statut privilégié pour un membre est celui de cadre. Le CMSAI se rencontre minimalement deux fois par année.

Les membres du CMSAI sont :

- le sous-ministre ou son représentant, président du comité;
- le responsable de l'accès à l'information et de la protection des renseignements personnels (RAIPRP);
- le responsable de la sécurité de l'information (RSI), secrétaire du comité;
- le responsable de la gestion documentaire (RGD);
- pour chacun des secteurs¹⁴,
un représentant sectoriel de la SI et des mandataires de ce secteur;
- le responsable de la gestion des TI au SCSP;
- le responsable de la gestion des TI à Foncier Québec;
- le directeur de la Direction de l'évaluation et de la vérification;
- un représentant de la Direction des communications.

Les conseillers sont :

- le conseiller en accès à l'information;
- le conseiller en protection des renseignements personnels;
- un conseiller juridique.

En fonction des sujets ou des besoins exprimés par les membres du CMSAI, d'autres intervenants peuvent être invités à participer à une rencontre, dont :

- le directeur de la Direction des ressources matérielles;
- le directeur de la Direction des ressources humaines.

¹⁴ L'Agence de l'efficacité énergétique, qui utilise les infrastructures technologiques du MRNF, est également représenté sur le comité.

Annexe 3 – Les sous-comités du CMSAI

A3.1. Sous-comité de la protection des renseignements personnels

En vertu des articles 7 à 9 du *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels* (c. A-2.1, r.0.2), le Ministère doit informer et consulter le Comité ministériel de sécurité et d'accès à l'information (CMSAI) à l'égard de projets concernant les systèmes d'information, les sondages et la vidéosurveillance afin d'apprécier les possibles conséquences en matière de protection des renseignements personnels (PRP). Pour soutenir le CMSAI dans la mise en œuvre de ces prescriptions, le Sous-comité de la PRP a le mandat de répondre aux obligations en matière de PRP prescrites par le Règlement.

Ce sous-comité se rencontre environ huit fois par année et il doit :

- analyser les 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 et recommander, parmi ces projets, ceux qui doivent être encadrés par des mesures particulières de PRP;
- analyser et approuver les projets de sondages, recommander des mesures particulières à respecter en matière de PRP relatives au sondage recueillant ou utilisant des renseignements personnels;
- analyser les projets de vidéosurveillance et recommander des mesures particulières à respecter en matière de PRP relatives à une technologie de vidéosurveillance;
- rendre compte périodiquement de ces travaux au CMSAI.

Les membres de ce sous-comité de la PRP sont :

- le responsable de l'accès à l'information et de la protection des renseignements personnels (RAIPRP), président du comité;
- le responsable de la sécurité de l'information (RSI);
- le responsable de la gestion documentaire (RGD);
- le conseiller en protection des renseignements personnels, secrétaire du comité;
- le conseiller en accès à l'information;
- lorsque requis, et selon la provenance des projets technologiques soumis, un représentant du responsable de la gestion des TI au SCSP ou à Foncier Québec.

Selon les projets qui seront présentés, d'autres intervenants pourront être invités à participer à une rencontre du Sous-comité de la PRP.