

Politique concernant 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	17 mars 2008	Benoit Lessard	<ul style="list-style-type: none"> ▪ Version préliminaire pour commentaires du dir. BSMS et du conseiller en protection des renseignements personnels (PRP)
0.2	4 avril 2008	Benoit Lessard	<ul style="list-style-type: none"> ▪ Version intégrant les commentaires du dir. BSMS et du conseiller en PRP ▪ Version préliminaire pour commentaires de la DGTI et d'intervenants de Foncier Québec
0.3	9 mai 2008	Benoit Lessard	<ul style="list-style-type: none"> ▪ Version intégrant les commentaires de la DGTI et d'intervenants de Foncier Québec ▪ Version pour commentaires des membres du CMSAI et pour une révision linguistique
0.4	12 juin 2008	Benoit Lessard	<ul style="list-style-type: none"> ▪ Version intégrant les commentaires des membres du CMSAI et les corrections linguistiques retenues ▪ Version pour recommandation d'approbation par les membres du CMSAI
0.5	24 juillet 2008	Benoit Lessard	<ul style="list-style-type: none"> ▪ Version pour adoption par les membres du CD-MRNF
1.0	5 novembre 2008	Benoit Lessard	<ul style="list-style-type: none"> ▪ Document approuvé et 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 cette Politique a été inspirée notamment par :

- le cadre légal et normatif en vigueur;
- les différents guides produits par le gouvernement du Québec, dont le *Guide pour l'élaboration d'une politique de sécurité de l'information numérique et des échanges électroniques* (SGQRI 34), version 1.0 de juillet 2003;
- les politiques reçues 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, 4^e Avenue Ouest, bureau A 303
 Québec (Québec) G1H 6R1

© Gouvernement du Québec

Table des matières

1.	INTRODUCTION.....	1
1.1.	DÉFINITION DE LA SÉCURITÉ DE L'INFORMATION (SI).....	2
1.2.	OBJECTIFS DE LA SI.....	2
2.	CADRE ADMINISTRATIF DE LA SI.....	3
3.	CHAMP D'APPLICATION.....	5
3.1.	OBJET DE LA POLITIQUE.....	5
3.2.	INFORMATIONS VISÉES.....	5
3.3.	PERSONNES VISÉES - UTILISATEURS.....	5
3.4.	ACTIVITÉS VISÉES.....	5
4.	PRINCIPES DIRECTEURS.....	6
5.	ÉNONCÉS DE SÉCURITÉ.....	7
5.1.	ASSURER LA PROTECTION DE L'INFORMATION DURANT TOUT SON CYCLE DE VIE.....	7
5.2.	PROTÉGER LES RENSEIGNEMENTS CONFIDENTIELS.....	7
5.3.	PROTÉGER L'INTÉGRITÉ, LES PREUVES ET LA VALEUR JURIDIQUE.....	8
5.4.	ASSURER LA GESTION DES DOCUMENTS ET LEUR DISPOSITION.....	8
5.5.	GÉRER LA DISPONIBILITÉ ET ASSURER LA CONTINUITÉ DES ACTIVITÉS.....	8
5.6.	ÉVALUER ET PRENDRE EN COMPTE LES RISQUES.....	8
5.7.	GÉRER LA COHÉRENCE DES MESURES.....	9
5.8.	ÉTABLIR LA RESPONSABILITÉ INDIVIDUELLE ET COLLECTIVE.....	9
5.9.	ASSURER LA SÉPARATION DES TÂCHES INCOMPATIBLES.....	9
5.10.	ASSURER, EN CONTINU, LA FORMATION ET LA SENSIBILISATION.....	9
5.11.	EXERCER UN DROIT DE REGARD ET D'INTERVENTION.....	10
5.12.	EXERCER L'HABILITATION SÉCURITAIRE.....	10
5.13.	ASSURER LA CONFORMITÉ AUX NORMES ET AUX STANDARDS.....	10
5.14.	RESPECTER LE DROIT DE PROPRIÉTÉ INTELLECTUELLE.....	10
5.15.	MESURES D'EXCEPTION.....	10
6.	RÔLES ET RESPONSABILITÉS.....	11
6.1.	SOUS-MINISTRE.....	11
6.2.	RESPONSABLE DE LA SÉCURITÉ DE L'INFORMATION (RSI).....	11
6.3.	SOUS-MINISTRES ASSOCIÉS.....	12
6.4.	DIRECTION DE L'ÉVALUATION ET DE LA VÉRIFICATION (DEV).....	12
6.5.	MANDATAIRE D'ÉLÉMENTS DE L'ACTIF INFORMATIONNEL.....	12
7.	STRUCTURE DE COORDINATION ET DE CONCERTATION.....	13
7.1.	COMITÉ DE DIRECTION (CD-MRNF).....	13
7.2.	COMITÉ MINISTÉRIEL DE SÉCURITÉ ET D'ACCÈS À L'INFORMATION (CMSAI).....	13
8.	DISPOSITIONS FINALES.....	14
8.1.	SANCTIONS.....	14
8.2.	MISE EN ŒUVRE, SUIVI ET RÉVISION.....	14
8.3.	APPROBATION ET DATE D'ENTRÉE EN VIGUEUR.....	14
	ANNEXE 1 – CADRE LÉGAL ET ADMINISTRATIF.....	15
	ANNEXE 2 – GLOSSAIRE.....	17
	ANNEXE 3 – EXIGENCES DES NORMES DU SCP (PCI DSS).....	23

1. Introduction

En vertu de l'article 1 et 11.1 de la *Loi sur le ministère des Ressources naturelles et de la Faune* (L.R.Q., c. M-25.2), le ministère des Ressources naturelles et de la Faune (MRNF) a pour mission d'assurer, dans une perspective de développement durable et de gestion intégrée, la conservation et la mise en valeur des ressources naturelles, dont la faune et son habitat, ainsi que des terres du domaine de l'État. Il intervient dans les domaines d'activité suivants : le territoire, la faune, les forêts, les mines, l'énergie et l'information foncière.

Le MRNF emmagasine, traite et communique de l'information sous plusieurs formes afin de mener à bien sa mission. L'information possède, en outre, une valeur légale, administrative, économique ou patrimoniale. Cette information étant essentielle à ces activités, il convient de mettre en oeuvre un ensemble cohérent de processus et de mécanismes afin d'assurer la protection durant tout son cycle de vie, c'est-à-dire dès sa conception jusqu'à son aliénation, sa destruction ou son versement à Bibliothèque et Archives nationales du Québec.

La *Directive sur la sécurité de l'information gouvernementale* (C.T. 203560 du 11 avril 2006) énonce les objectifs et les principes directeurs en matière de sécurité de l'information gouvernementale et détermine les responsabilités des ministères et organismes. Principalement, elle demande à chaque ministère et organisme de définir clairement les valeurs organisationnelles et les orientations en matière de sécurité au sein de son organisation, de les faire partager à l'ensemble de son personnel et de les communiquer à ses partenaires afin de s'assurer de leur respect.

Par ailleurs, plusieurs lois imposent des exigences en matière de sécurité de l'information, particulièrement pour la protection des renseignements personnels¹ ainsi qu'en matière de diffusion, de divulgation et d'intégrité de l'information détenue par le MRNF. Une liste non exhaustive est présentée à l'annexe 1.

Pour ces raisons, la sécurité de l'information revêt une importance stratégique. Elle fait donc l'objet d'un ensemble intégré de mesures précises qui s'articulent à l'intérieur d'une structure bien définie dont la présente Politique constitue la pierre d'assise. La *Politique concernant la sécurité de l'information* exprime clairement les objectifs, les principes directeurs, les énoncés de sécurité et les principaux rôles en la matière pour établir la structure de gouvernance de la sécurité de l'information.

¹ Article 63.1 de la *Loi sur l'accès aux documents des organismes publics et la protection des renseignements personnels* (L.R.Q., c. A-2.1)

1.1. 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 activités et celle de la protection des personnes et des biens; et les façons d'être, l'éthique.

D'autres définitions sont présentées au glossaire à l'annexe 2.

1.2. 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.

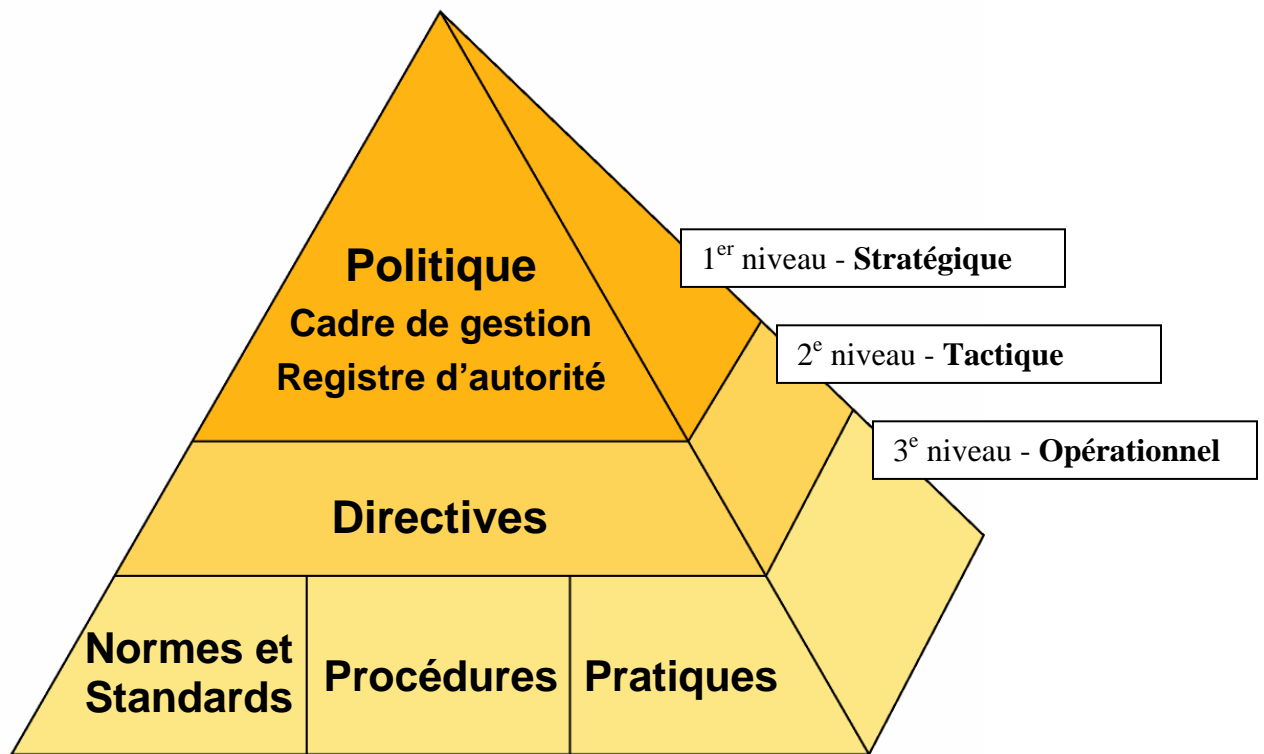
En tenant compte des risques et de leurs impacts pour le Ministère et le gouvernement, les mesures de sécurité à maintenir ou à mettre en place doivent être proportionnelles à la valeur de l'information à protéger. Elles visent à :

- **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 voulue;
- **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.

2. Cadre administratif de la SI

Le cadre administratif de la SI comporte différents documents de nature stratégique, tactique et opérationnel. La présente Politique établit la structure de ce cadre et énonce les orientations stratégiques en la matière afin notamment de baliser la production et la mise à jour de ses différents documents. La documentation supportant ce cadre administratif se doit d'être évolutive afin de permettre les ajustements nécessaires tant au plan stratégique vers le plan opérationnel que l'inverse.

Le schéma ci-dessous représente le cadre administratif de la SI.



1^{er} niveau - Stratégique

La *Politique concernant la sécurité de l'information*, le *Cadre de gestion de la sécurité de l'information* et le *Registre d'autorité de la sécurité de l'information* sont les assises de la gouvernance en SI et permettent d'établir et de promulguer l'encadrement stratégique, de structurer cette gouvernance et de nommer les intervenants pour chacun des rôles.

2^e niveau - Tactique

En appui aux constituants du niveau stratégique, les directives permettent de développer et de préciser les éléments de sécurité. Elles déterminent, par des mesures concrètes, la façon de procéder en vue d'assurer la SI dans des domaines d'application particuliers.

3^e niveau - Opérationnel

Normes et standards - S'inspirer ou se conformer à des normes et standards généralement reconnus permet de réduire la complexité des environnements et des opérations en uniformisant les éléments constituant un univers informationnel au sein d'une organisation. Les normes et standards fixent les bases architecturales des systèmes et fournissent un dénominateur commun pour l'évolution des éléments de l'actif informationnel.

Procédures - Une procédure, c'est l'ensemble des étapes à franchir ou à réaliser, des moyens à prendre et des méthodes à suivre dans l'exécution d'une tâche ou d'une activité.

Pratiques - Les pratiques sont basées sur des méthodes et des procédures qui découlent de normes explicites (lois, politiques, règlements, directives, etc.) et de normes implicites. Étant donné que l'implantation de mesures de sécurité se fait généralement sur la base de tâches particulières à accomplir ou de zones d'activité opérationnelles spécifiques, les pratiques seront le plus souvent transversales, c'est-à-dire qu'elles seront reliées à plusieurs normes explicites.

3. Champ d'application

3.1. Objet de la Politique

La présente Politique a pour objet d'établir et de promulguer l'encadrement stratégique de la SI au MRNF, et ce, dans l'intention :

- de se conformer aux lois et aux directives en vigueur;
- de mettre en œuvre les mesures de sécurité nécessaires pour atteindre les objectifs de la sécurité de l'information;
- de se conformer aux normes et aux standards qu'il a choisi de mettre en œuvre.

3.2. Informations visées

Cette Politique s'applique aux catégories d'information suivantes :

- l'information appartenant au MRNF et exploitée par lui;
- l'information appartenant au MRNF et exploitée ou détenue par un partenaire, un fournisseur de produits/services ou un autre intervenant;
- l'information appartenant à un partenaire, à un fournisseur de produits/services ou à un autre intervenant et exploitée par lui au profit du MRNF;
- l'information n'appartenant pas au MRNF et détenue par lui.

3.3. Personnes visées - Utilisateurs

Cette Politique s'applique à toutes les 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. Ces personnes sont désignées dans la présente Politique sous le vocable « utilisateur ».

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.

3.4. Activités visées

Toutes les activités impliquant la manipulation ou l'utilisation de l'information appartenant au MRNF, peu importe sa forme, sont visées par la présente Politique, que celles-ci soient conduites dans ses locaux ou dans un autre lieu.

4. Principes directeurs

En plus de maintenir et même, de rehausser la confiance de la clientèle à l'égard des services que le MRNF rend et de contribuer à la réalisation de sa mission, la SI au Ministère doit viser à atteindre un niveau de sécurité jugé acceptable afin notamment d'assurer la pérennité d'une information fiable.

Pour ce faire, le MRNF doit assurer la sécurité de ses informations conformément aux principes directeurs suivants :

- **Responsabilité et imputabilité** : Les responsabilités en matière de sécurité de l'information sont attribuées clairement à tous les niveaux de l'organisation. Le processus de gestion intégrée de la sécurité de l'information est mis en place notamment pour permettre une reddition de comptes adéquate.
- **Évolution et universalité** : Les pratiques et les mesures de sécurité adoptées par le MRNF sont réévaluées périodiquement afin de tenir compte des changements juridiques, organisationnels, humains et technologiques ainsi que de l'évolution des menaces et des risques. Celles-ci doivent correspondre, dans la mesure du possible, à des façons de faire reconnues et généralement utilisées au gouvernement du Québec de même qu'à l'échelle nationale et internationale.
- **Éthique** : La gestion de la sécurité de l'information est soutenue par une démarche éthique. L'éthique étant un processus de réflexion continu sur le sens et les conséquences multiples des actions, elle permet de soutenir la prise de décision, d'assurer la régulation des conduites et la responsabilisation individuelle.

5. Énoncés de sécurité

Les énoncés suivants constituent les orientations stratégiques que se donne le MRNF en matière de SI.

5.1. Assurer la protection de l'information durant tout son cycle de vie

La protection de l'information est fondée sur les énoncés généraux suivants :

- L'information détenue par le MRNF est essentielle à sa mission ainsi qu'à ses opérations courantes et doit faire l'objet d'une utilisation et d'une protection adéquates durant tout son cycle de vie.

Le niveau de protection accordé est établi en fonction de la sensibilité et des risques d'accident, d'erreur ou de malveillance auxquels l'information est exposée. Également, l'établissement de ce niveau de protection tient compte de l'ensemble des moyens, biens et lieux qui permettent d'avoir accès à cette information.

- La protection de l'information du MRNF s'appuie sur l'engagement continu de l'ensemble des utilisateurs. Chacun a l'obligation de protéger l'information et les supports mis à sa disposition en l'utilisant avec discernement et aux seules fins prévues.
- L'information détenue par le MRNF doit être protégée selon les exigences qui y sont liées pour assurer sa disponibilité, son intégrité et sa confidentialité.
- L'information produite ou utilisée dans un processus est assignée à un mandataire, catégorisée et inventoriée.
- Les rôles et les responsabilités en matière de sécurité de l'information doivent être établis dans un cadre de gestion. Les rôles doivent être attribués et consignés dans un registre.

5.2. Protéger les renseignements confidentiels

Le MRNF doit prendre les mesures de sécurité propres à assurer la protection des renseignements confidentiels collectés, utilisés, communiqués ou conservés ainsi que ceux à détruire et qui sont raisonnables compte tenu, entre autres de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support. Sont notamment confidentiels les renseignements personnels et les renseignements ayant des incidences sur l'économie, au sens 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) ainsi que tout renseignement dont la divulgation aurait notamment pour effet de réduire l'efficacité d'un dispositif de sécurité.

5.3. Protéger l'intégrité, les preuves et la valeur juridique

Le MRNF doit maintenir l'intégrité de tout document servant à l'établissement de la preuve d'un acte juridique ou d'un fait nonobstant l'interchangeabilité du support afin de préserver son admissibilité éventuelle devant les tribunaux. À cette fin, les processus, procédés et mécanismes qui encadrent la copie, le classement, la saisie, la transmission ou le transfert de support d'un document doivent assurer le maintien de son intégrité et, conséquemment, de sa valeur probante.

5.4. Assurer la gestion des documents et leur disposition

Le MRNF est assujéti, entre autres, aux 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. Pour y répondre, et aussi assurer la conservation et la gestion intégrée des documents (GID), le MRNF doit planifier et encadrer la création, l'utilisation, la conservation et la disposition finale des documents, et ce, peu importe leur support.

Les documents ainsi que les équipements qui sont destinés au rebut, déclarés en bien excédentaire ou confiés à un fournisseur de services pour qu'il procède entre autres à leur entretien, à leur recyclage ou à leur destruction, doivent respecter l'ensemble des directives en vigueur quant à leurs destruction ou disposition. De plus, l'article 63.1 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) impose que les ministères et organismes se dotent de mesures de sécurité afin de disposer de documents comportant des renseignements personnels.

5.5. Gérer la disponibilité et assurer la continuité des activités

Toute information doit être accessible et utilisable en temps voulu par une personne autorisée, et ce, tout au long du cycle de vie de l'information.

Le MRNF doit s'assurer de la continuité des activités nécessaires à la réalisation de sa mission dans un délai raisonnable lors d'un sinistre ou d'un incident majeur affectant la disponibilité de l'information jugée essentielle et stratégique.

5.6. Évaluer et prendre en compte les risques

Au MRNF, le choix des mesures de sécurité s'appuie sur l'identification et l'évaluation périodique des risques qui menacent l'information. En outre, une évaluation des risques et le choix de mesures de sécurité doivent être effectués dès le début des études visant la conception, l'acquisition ou un changement important aux processus d'affaires, aux systèmes d'information, aux infrastructures ou aux supports de documents.

5.7. Gérer la cohérence des mesures

La SI doit reposer sur une approche cohérente et intégrée qui tient compte des aspects juridique, humain, organisationnel et technologique. Celle-ci nécessite la mise en oeuvre d'un ensemble de mesures coordonnées de prévention, de dissuasion, de détection, de correction et de sanction.

5.8. Établir la responsabilité individuelle et collective

L'atteinte d'un niveau optimal en SI nécessite l'adhésion à une vision et à une compréhension communes de la sécurité et doit s'appuyer sur l'engagement continu des utilisateurs, tels que définis à l'article 3.3.

Chacun a l'obligation de protéger l'information qui est mise à sa disposition en l'utilisant avec discernement et aux seules fins prévues. Il en va de même pour l'ensemble des moyens, biens et lieux qui permettent d'avoir accès à cette information. La responsabilité de chacun en matière de sécurité de l'information est à la fois individuelle et collective.

Chacun a l'obligation de signaler, sans tarder, tout acte susceptible de représenter une atteinte réelle ou présumée à la sécurité de l'information, tel que le vol, l'intrusion, les dommages, la fraude, l'accès non autorisé, l'indiscrétion et l'utilisation abusive d'un élément de l'actif informationnel.

5.9. Assurer la séparation des tâches incompatibles

La séparation des tâches incompatibles consiste à s'assurer que certaines tâches ou fonctions complémentaires sont exécutées par différentes personnes. Elle permet de prévenir et de détecter des erreurs ou des fraudes, puis d'éviter de placer ces personnes dans une situation où elles pourraient les dissimuler. La séparation des tâches incompatibles doit être un élément clé lors de l'élaboration ou la révision des processus concernant les utilisateurs.

5.10. Assurer, en continu, la formation et la sensibilisation

L'aspect humain étant une des pierres angulaires de la protection de l'information, la formation et la sensibilisation à la SI de manière continue sont essentielles pour quiconque a accès à l'information appartenant au MRNF. Il importe de les sensibiliser aux conséquences d'une atteinte à la sécurité ainsi qu'aux rôles et aux obligations de tous pour assurer la protection de l'information et une utilisation correcte de celle-ci.

5.11. Exercer un droit de regard et d'intervention

Le Ministère a un droit de regard et d'intervention sur l'utilisation de l'information ou des moyens, des biens et des lieux qui permettent d'avoir accès à l'information ou d'en assurer la sécurité. Ce droit de regard sera exercé conformément au cadre légal et administratif applicable au MRNF, notamment dans le respect de la vie privée.

5.12. Exercer l'habilitation sécuritaire

Le MRNF affirme son droit d'exercer de l'habilitation sécuritaire concernant les personnes qui occupent ou occuperont des fonctions clés dans la gestion et l'utilisation de l'information qui lui appartient.

Ce contrôle de sécurité doit être réalisé dans le respect des lois, règlements, politiques et conventions collectives applicables ainsi que dans la déférence des personnes visées. Par ailleurs, le Ministère énonce son droit d'inclure des clauses permettant d'obtenir des habilitations sécuritaires des individus liés par des conventions.

5.13. Assurer la conformité aux normes et aux standards

Le MRNF peut choisir de respecter des normes et des standards et de s'y conformer. Il a aussi l'obligation de se conformer aux normes et aux standards qu'il a acceptés dans le cadre d'une convention.

L'une de ces normes est : *Normes de sécurité des données du secteur des cartes de paiement* (normes du SCP²), communément appelé PCI DSS³. C'est dans le cadre d'une convention et à titre de marchand que le MRNF doit obtenir et maintenir la certification aux normes du SCP. Un résumé des exigences de ces normes est présenté à l'annexe 3.

5.14. Respecter le droit de propriété intellectuelle

Le MRNF et chacun des utilisateurs doivent se conformer aux exigences légales portant sur l'utilisation de produits à l'égard desquels il pourrait y avoir un droit de propriété intellectuelle.

5.15. Mesures d'exception

Aucune dérogation à la présente Politique ainsi qu'aux documents afférents n'est permise sans l'autorisation écrite du sous-ministre ou de son représentant.

² La norme du SCP est administrée par le Conseil sur les normes de sécurité du SCP (PCI Security Standards Council)

³ PCI-DSS (*Payment Card Industry - Data Security Standard*)

6. Rôles et responsabilités

Les rôles et responsabilités en matière de SI doivent être définis pour les niveaux de gestion stratégique, tactique et opérationnel, et ce, pour les éléments pris en compte par la sécurité de l'information, tels que défini à la section 1.1 de cette Politique. Ces éléments sont : l'accès à l'information et la protection des renseignements personnels, la continuité des activités, l'éthique, la gestion documentaire, la sécurité des personnes et des biens et les technologies de l'information.

La présente section expose sommairement les responsabilités des rôles stratégiques ou d'importance, tandis que l'ensemble des rôles sont décrits en détail dans le *Cadre de gestion de la sécurité de l'information*.

6.1. 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 cette 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) ainsi qu'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.

6.2. 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.

6.3. 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. Ils doivent notamment :

- s'assurer de la mise en œuvre de la SI dans leurs secteurs;
- soutenir dans leurs responsabilités les mandataires des éléments de l'actif informationnel de leur secteur;
- désigner un représentant sectoriel à titre de membre du Comité ministériel de sécurité et d'accès à l'information;
- commenter les éléments de gouvernance de la SI.

6.4. 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 présente Politique et des documents afférents. À cette fin, elle doit notamment :

- effectuer des vérifications indépendantes et objectives des éléments constituant la SI dans un contexte de gestion intégrée des risques 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;
- faire le lien avec le Vérificateur général du Québec.

6.5. Mandataire 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 d'un 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*.

Le mandataire doit principalement 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.

7. Structure de coordination et de concertation

La structure de coordination et de concertation doit permettre d'établir une vision commune de la SI en vue d'assurer la cohérence et l'intégration des préoccupations et des interventions en la matière au MRNF, et ce, tant au plan stratégique, tactique qu'opérationnel. L'objectif commun des comités consiste à soutenir le sous-ministre, le RSI et tout autre responsable dans leurs fonctions.

La présente section expose sommairement les responsabilités du Comité de direction du Ministère et celles du Comité ministériel de sécurité et d'accès à l'information, tandis que le détail de la structure de coordination et de concertation est décrit dans le *Cadre de gestion de la sécurité de l'information*.

7.1. 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 lui sont présentés.

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

Présidé par le sous-ministre ou son représentant, le CMSAI a trois mandats :

- soutenir le sous-ministre dans l'exercice de ses responsabilités et obligations en matière de SI, incluant celles en accès à l'information et en protection des renseignements personnels;
- 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;
- 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.

8. Dispositions finales

Le présent document remplace la *Politique de sécurité de l'information électronique et des actifs informationnels*, DSI, MRNF, 18 juin 1998.

8.1. Sanctions

Lorsqu'un utilisateur contrevient à la *Politique concernant la sécurité de l'information* ou tout autre élément (directives, procédures, pratiques, normes et standards) découlant de cette Politique, il s'expose à des mesures administratives, disciplinaires ou légales en fonction de la gravité et des conséquences de son geste.

Ces mesures peuvent inclure le retrait des privilèges relatifs à l'accès ou à l'utilisation d'un élément de l'actif informationnel, l'avertissement, la réprimande, la suspension, le congédiement ou autre, et ce, conformément aux lois et aux dispositions des conventions collectives ou autres conventions.

Aussi, le MRNF peut référer à ses procureurs ou à tout corps de police compétent les informations colligées qui le portent à croire qu'une infraction à toute loi ou à tout règlement en vigueur a été commise.

8.2. Mise en œuvre, suivi et révision

La coordination de la mise en œuvre de cette Politique 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 de SI du Ministère, la présente Politique doit être révisée annuellement après son entrée en vigueur ou lors de changements significatifs qui pourraient l'affecter.

8.3. Approbation et date d'entrée en vigueur

La présente *Politique concernant la sécurité de l'information* est approuvée et entre en vigueur à la date de la signature par le sous-ministre.

Original signé

2008/11/05

Normand Bergeron
Sous-ministre

Date

Annexe 1 – Cadre légal et administratif

Sans être exhaustive, la présente Politique s'appuie sur la liste des lois et directives suivantes:

- Charte des droits et libertés de la personne du Québec (L.R.Q., c. C-12);
- Charte canadienne des droits et libertés (1982)
L.R.C. (1985), App. II, no. 44;
- Loi sur le ministère des Ressources naturelles et de la Faune
(L.R.Q., c. M-25.2);
- Loi sur le droit d'auteur (L.R. 1985, c. C-42);
- Loi sur la sécurité civile (L.R.Q., c. S-2.3);
- Loi concernant le cadre juridique des technologies de l'information
(L.R.Q., c. C-1.1);
- Loi sur l'accès aux documents des organismes publics et sur la protection
des renseignements personnels (L.R.Q., c. A-2.1);
- Loi sur les archives (L.R.Q., c. A-21.1);
- Loi sur l'administration publique (L.R.Q., c. A-6.01);
- Loi sur la fonction publique (L.R.Q., c. F-3.1.1);
- Loi sur l'administration financière (L.R.Q., c. A-6.001);
- Loi sur les marques de commerce (L.R. 1985 c. T-13);
- Code criminel (L.R. 1985, c. C-46);
- Code civil du Québec, C.c.Q.;
- Règlement sur l'éthique et la discipline dans la fonction publique
(L.R.Q., c. F-3.1.1, r.0.3);
- Règlement sur la diffusion de l'information et sur la protection des
renseignements personnels
(L.R.Q., c. A-2.1, a.16.1, 63.2 et 155 ; 2006, c. 22, a. 9 et 34);
- Directive sur la sécurité de l'information gouvernementale
(CT 203560 du 11 avril 2006);
- Directive sur l'utilisation éthique du courriel, d'un collecticiel, et des
services d'Internet par le personnel de la fonction publique
(CT 198872 du 1er octobre 2002);
- Directive concernant le traitement et la destruction de tout renseignement,
registre, donnée, logiciel, système d'exploitation ou autre bien protégé par
un droit d'auteur, emmagasiné sur un équipement micro-informatique ou
un support informatique amovible (CT 193953 du 19 octobre);

Annexe 2 – 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, 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.

Cycle de vie de l'information

Ensemble des étapes que franchit une 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 d'une organisation.

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.

Droit de propriété intellectuelle

Droit incorporel dont l'objet est une création de l'esprit. On reconnaît notamment les types de droits suivants : le droit d'auteur (incluant le droit moral), le brevet, le dessin industriel et la marque de commerce.

Fournisseur

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

Habilitation sécuritaire

C'est une appréciation sur l'intégrité et la fiabilité d'un candidat, d'un employé ou d'un consultant. Elle est demandée, obtenue ou validée par des vérifications ou des enquêtes de sécurité et elle doit être pertinente à la réalisation de la fonction de la personne ciblée.

Cette appréciation consiste à déterminer si la présence de certains antécédents peut comporter un risque ou une menace pour la sécurité d'État ou de ses institutions, la sécurité des personnes, des biens et des informations. Elle se fait en évaluant s'il y a un lien entre les informations recueillies concernant la personne et la fonction qu'elle est appelée à remplir. La présence d'un tel lien peut constituer un empêchement. Cette appréciation tient également compte de la valeur des biens et informations à protéger et des impacts d'un bris d'intégrité, de disponibilité ou de confidentialité sur la sécurité et sur la confiance du public dans l'organisation.

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.

Plans de sécurité

Inspiré de la méthode MÉHARI⁴, 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);
Les POS sont élaborés pour chacune des unités administratives concernées. 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.
- 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.

Processus d'affaires

Suite cohérente d'activités et d'opérations commerciales qu'une organisation entretient avec différents intervenants, 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.

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.

⁴ Méthode Harmonisée de Risques Informatiques, CLUSIF (www.clusif.asso.fr)

Renseignement confidentiel

Renseignement secret, stratégique ou personnel dont la divulgation non autorisée risquerait de causer un préjudice au Ministère, à son personnel ou à sa clientèle.

Sans limiter la généralité de ce qui précède, il inclut notamment : le secret industriel; le renseignement industriel, scientifique, technique, financier, commercial et syndical; le renseignement ayant des incidences sur les relations interministérielles, intergouvernementales ou internationales; le renseignement ayant des incidences sur la sécurité ou l'administration de la justice; le renseignement sur les décisions administratives ou politiques; le renseignement ayant les incidences sur la vérification; le renseignement visé par le secret professionnel.

Renseignement personnel

Sont personnels les renseignements qui concernent une personne physique et permettant de l'identifier.

Renseignement sensible

Tout renseignement considéré comme confidentiel, stratégique, essentiel, critique, indispensable ou vital pour ses opérations, et dont la divulgation, l'altération, la perte ou la destruction est susceptible de porter un préjudice au MRNF, à son personnel ou à sa clientèle, ses partenaires et ses fournisseurs.

Ressource informationnelle

Ressource utilisée par une organisation, dans le cadre de ses activités de traitement de l'information, pour mener à bien sa mission, pour la prise de décision, ou encore pour la résolution de problèmes.

Une ressource informationnelle peut être une ressource humaine, matérielle ou financière directement affectée à la gestion, à l'acquisition, au développement, à l'entretien, à l'exploitation, à l'accès, à l'utilisation, à la protection, à la conservation et à la destruction des éléments d'information. Une ressource peut notamment être une personne, un document, quel que soit son support, un système d'information et un processus d'affaires

La plupart du temps, les termes ressources informationnelles, ressource d'information et ressource en information sont utilisés au pluriel (ressources informationnelles, ressources d'information et ressources en information). Ils désignent alors un ensemble de ressources qui peuvent être répertoriées dans l'actif informationnel de l'organisation.

Sécurité des technologies de l'information (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 physique

Aspect de la sécurité qui traite des mesures physiques prises pour assurer la protection des personnes et des biens, empêcher notamment tout accès non autorisé aux équipements, installations et documents et à les protéger contre toute forme de menace physique, accidentelle ou humaine.

La sécurité physique porte aussi bien sur le centre informatique lui-même et son périmètre, sur les bâtiments et locaux tels que bureaux, salles informatiques, locaux techniques, que sur les matériels de servitude, sur l'équipement informatique et sur les supports informatiques tels que les disques, disquettes et bandes magnétiques, sans oublier les listages et la documentation.

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 3 – Exigences des normes du SCP (PCI DSS)

Le Conseil sur les normes de sécurité du secteur des cartes de paiement prescrit la conformité aux normes du SCP⁵ (communément appelé PCI DSS⁶) pour les marchands et fournisseurs de services dont les systèmes mémorisent, traitent ou transmettent des données provenant des cartes de paiement de leurs clients.

Pour répondre à cette obligation, ils doivent adopter des contrôles et des processus de sécurité de l'information pour assurer la sécurité des données et répondre aux 12 exigences des normes du SCP. Ceux-ci s'organisent en 6 groupes logiques liés nommés « objectifs de contrôle ». En plus, une révision des systèmes et procédures de sécurité doit être réalisée annuellement conformément aux exigences des normes du SCP.

Mettre en place et gérer un réseau sécurisé

- Exigence 1 : Installer et gérer une configuration de pare-feu afin de protéger les données des titulaires de carte;
- Exigence 2 : Ne pas utiliser les paramètres par défaut du fournisseur pour les mots de passe et les autres paramètres de sécurité du système;

Protéger les données des titulaires de carte

- Exigence 3 : Protéger les données des titulaires de carte stockées;
- Exigence 4 : Chiffrer la transmission des données des titulaires de carte sur les réseaux publics ouverts;

Disposer d'un programme de gestion de la vulnérabilité

- Exigence 5 : Utiliser et mettre à jour régulièrement un logiciel antivirus;
- Exigence 6 : Développer et gérer des applications et systèmes sécurisés;

Mettre en oeuvre des mesures de contrôle d'accès efficaces

- Exigence 7 : Limiter l'accès aux données des porteurs de carte aux cas de nécessité professionnelle absolue;
- Exigence 8 : Attribuer une identité d'utilisateur unique à chaque personne disposant d'un accès informatique;
- Exigence 9 : Limiter l'accès physique aux données des titulaires de carte;

Surveiller et tester régulièrement les réseaux

- Exigence 10 : Suivre et surveiller tous les accès aux ressources du réseau et aux données des titulaires de carte;
- Exigence 11 : Tester régulièrement les systèmes et procédures de sécurité;

Disposer d'une politique en matière de sécurité de l'information

- Exigence 12 : Disposer d'une politique régissant la sécurité de l'information.

⁵ Normes de sécurité des données du secteur des cartes de paiement (SCP), administrées par le Conseil sur les normes de sécurité du SCP (PCI Security Standards Council)

⁶ PCI-DSS (*Payment Card Industry - Data Security Standard*)