POLITIQUE DE SÉCURITÉ DE L'INFORMATION

VERSION 1.0

MAI 2015

Énergie et Ressources naturelles
Québec

Historique de validation du document

Version	Date	Description des modifications
0.1	02 mars 2015	Version préliminaire pour commentaires de la ROSI
0.2	03 mars 2015	Version préliminaire pour commentaire DGARI + DGTA
0.3	06 mars 2015	Version intégrant les commentaires DGARI + DGTA
0.4	09 mars 2015	Version intégrant les commentaires de la ROSI
0.5	17 mars 2015	Version intégrant les commentaires de la secrétaire générale, la DRMGC et la DEVI
0.6	27 mars 2015	Version intégrant les commentaires du Comité chargé de la sécurité de l'information
0.7	21 avril 2015	Révision linguistique
1.0	10 mai 2015	Document approuvé et signé par le sous-ministre

Les documents ayant servi à élaborer cette politique sont les suivants :

- Le Guide d'élaboration d'une politique de sécurité de l'information (2014) élaboré par le Secrétariat du Conseil du trésor;

- Politiques en sécurité de l'information du ministère des Ressources naturelles et de la Faune (2009), du ministère de l'Emploi et de la Solidarité sociale (2009), du ministère des Transports (2004), de la Chambre des notaires (2011);

- Projets de politiques du Secrétariat du Conseil du Trésor, du ministère du Conseil Exécutif et du ministère de l'Enseignement supérieur, de la Recherche et de la Science.

NOTE : Le générique masculin dans ce document est utilisé sans aucune discrimination et à seule fin d'alléger le texte et d'en faciliter la lecture.

TABLE DES MATIÈRES

1. Préambule

Le ministère de l'Énergie et des Ressources naturelles (ci-après « Ministère ») a pour mission « d'assurer la gestion et soutenir la mise en valeur des ressources énergétiques et minières ainsi que du territoire du Québec, dans une perspective de développement durable ».

Afin de bien mener sa mission, le Ministère collecte, utilise, conserve, traite et communique de l'information sous plusieurs formes. La valeur légale, administrative, économique ou patrimoniale de cette information justifie sa protection durant tout son cycle de vie.

Compte tenu de la nature hautement sensible de l'information traitée par le Ministère, la sécurité de l'information revêt une importance capitale et doit faire l'objet d'un ensemble intégré de mesures qui s'articulent à l'intérieur d'une structure de gouvernance bien définie.

Cette politique de sécurité de l'information (ci-après « politique ») constitue la pierre d'assise de la gouvernance du Ministère en la matière et incarne sa vision. Elle décrit les objectifs, les principes directeurs, le champ d'application, les orientations stratégiques ainsi que les rôles et les responsabilités des principaux acteurs.

2. Définitions

Les définitions des termes utilisés dans cette politique sont présentées à l'**annexe I**.

3. Cadre légal et administratif

C'est la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (L.R.Q., chapitre G-1.03) qui établit les règles de gouvernance et de gestion en matière de ressources informationnelles, y compris la sécurité de l'information. La Directive sur la sécurité de l'information gouvernementale, du Secrétariat du Conseil du trésor, adoptée par décret le 15 janvier 2014, énonce les objectifs et les principes directeurs en matière de sécurité de l'information gouvernementale et détermine les responsabilités des ministères et organismes publics.

Les lois et règlements sur lesquels s'appuie cette politique sont énumérés à l'**annexe II**.

4. Objectifs de la politique

La politique a pour objectif d'affirmer l'engagement du Ministère de s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information, quel que soit son support ou son moyen de communication. Plus précisément, elle a pour but :

- d'atteindre un degré adéquat de sécurité de l'information par une compréhension commune et l'engagement constant de tous les utilisateurs du Ministère, ainsi que de ses partenaires et fournisseurs;
- de soutenir la mise en œuvre des normes et standards internationaux;
- d'appuyer une démarche globale de gestion du risque et des incidents, laquelle sera actualisée et vérifiée de façon périodique;
- de renforcer la responsabilité collective et individuelle en diffusant l'information sur les principes directeurs et les bonnes pratiques en matière de sécurité de l'information.

5. Champ d'application

Cette politique s'applique à la sécurité de l'information, quelle que soit sa forme, numérique ou non. Elle couvre ainsi les domaines des technologies de l'information, de la sécurité physique ainsi que de la gestion documentaire.

5.1. Information et actifs informationnels visés

La politique de sécurité de l'information s'applique aux catégories d'information suivantes :

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

Elle vise l'information et les actifs informationnels détenus ou utilisés par le Ministère, qu'ils soient situés dans ses locaux ou dans les locaux d'un prestataire de services.

5.2. Personnes visées

Cette politique s'adresse aux utilisateurs, c'est-à-dire toute personne ayant accès à l'information et aux actifs informationnels du Ministère sans égard au statut d'emploi, y compris les employés contractuels et les personnes en prêts de service ainsi qu'à tous les partenaires, les fournisseurs ou autres intervenants.

5.3. Activités visées

Toute activité impliquant l'utilisation, la communication ou la conservation, sous quelle que forme que ce soit, d'une information ou d'un actif informationnel appartenant au Ministère, ou détenu par lui, est visée par la politique, qu'elle soit conduite dans ses locaux, dans un autre lieu ou à distance.

Cette politique s'applique dès la conception de l'information ou de l'actif informationnel et pendant le développement, la réalisation ou la modification d'un processus d'affaires d'un actif informationnel.

5.3.1. Développement informatique

Les exigences en matière de sécurité de l'information doivent être prises en considération dès le début des travaux menant à l'acquisition ou au développement d'un système d'information. Les mesures de protection requises doivent être appliquées tout au long du processus de conception du système.

Les environnements informatiques de développement et d'essai (acceptation) doivent être logiquement cloisonnés et séparés de l'environnement de production.

Tout nouveau système d'information ou toute évolution majeure d'un système d'information existant doit se voir assigner un détenteur, être catégorisé dans le registre d'autorité ministériel et faire l'objet, préalablement à sa mise en production, d'une vérification de sa sécurité au moyen de tests de vulnérabilité applicative et de tests d'intrusion le cas échéant.

5.3.2. Exploitation et administration des infrastructures des technologies de l'information

La sécurité des infrastructures des technologies de l'information doit être soutenue par des outils, des pratiques et des mesures de surveillance et de mise à jour continue des systèmes d'exploitation, des principaux logiciels et de l'équipement en usage au Ministère, y compris notamment :

- l'installation continue des mécanismes de correction mis sur le marché par les fournisseurs;
- une analyse annuelle des risques liés aux technologies de l'information;
- des tests de vulnérabilité récurrents et des tests d'intrusion annuels sur les réseaux interne et externe.

5.3.3. Destruction de l'équipement informatique

Les règles de destruction sécuritaire de tout équipement micro-informatique déclaré « bien meuble excédentaire » et de tout support informatique amovible[1] destiné au rebut ou confié à un fournisseur doivent s'appliquer en temps opportun et en conformité avec la 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 sur un support informatique amovible du Secrétariat du Conseil du trésor. Il en va de même de tout équipement micro-informatique ou support amovible confié à un fournisseur pour qu'il procède à sa réparation, à son entretien, à sa destruction ou à la récupération de l'information qui y est emmagasinée.

5.3.4. Gestion des documents et leur destruction

Le Ministère est soumis à la Loi sur les archives (L.R.Q., c.A-21.1) ainsi qu'aux politiques de gestion des documents établies par Bibliothèque et Archives nationales du Québec.

Il applique aussi la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q. chapitre A-2.1), notamment l'article 63.1 qui exige des mesures de sécurité relatives à la destruction des documents comportant des renseignements personnels.

5.3.5. Sécurité physique des édifices et des locaux

Cette politique concerne également la sécurité des lieux physiques. À cet égard, le Ministère établit une liste des lieux pour lesquels il a la responsabilité de la sécurité et s'assure de sa mise à jour périodiquement ou lors d'un changement organisationnel important.

De plus, lorsque le risque le justifie, les édifices et les locaux occupés par le Ministère, où sont traités ou hébergés l'information et les actifs informationnels de nature stratégique ou

[1] Inclut les disques durs des imprimantes multifonctions, l'équipement micro-informatique comme les portables, les téléphones mobiles, les tablettes numériques et les clés USB.

confidentielle, font l'objet de mesures de protection adéquates contre tout type de menaces[2].

6. Principes directeurs

6.1. Raison d'être de la sécurité de l'information

La sécurité de l'information a pour but de permettre de maintenir, voire rehausser, la confiance de la population à l'égard de l'État et des services qu'il rend, et de contribuer à la réalisation de la mission de l'État et à celle du Ministère. Elle a également pour but d'assurer la pérennité d'une information fiable.

6.2. Protection de l'information

La sécurité de l'information doit être assurée tout au long de son cycle de vie et les moyens mis en œuvre pour l'assurer doivent être proportionnels à sa valeur et aux risques auxquels elle est exposée. Ainsi, toute information que le Ministère détient, traite ou transmet doit faire l'objet de mesures de sécurité visant à :

- assurer la disponibilité de l'information de façon à ce qu'elle soit accessible en tout 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;
- limiter l'accès ou la divulgation aux seules personnes autorisées à en prendre connaissance, garantissant ainsi une utilisation stricte, contrôlée et confidentielle;
- permettre de confirmer l'identité d'une personne ou l'identification d'un document ou d'un dispositif (authentification);
- 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 (irrévocabilité).

Toute information confidentielle doit être préservée de toute divulgation, de tout accès ou de toute utilisation non autorisé. Sont notamment considérés comme confidentiels, au sens de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, les renseignements personnels ainsi que tout renseignement dont la divulgation aurait des incidences néfastes, notamment sur les relations

[2] Exemples de types de menaces : naturelles (foudre, inondations, etc.), accidentelles (incendie, bris de matériel, panne de courant, etc.), ou attribuables à la malveillance (intrusion, vol, vandalisme, etc.).

intergouvernementales, les négociations entre organismes publics, l'économie, les tiers relativement à leurs renseignements industriels, financiers, commerciaux, scientifiques ou techniques, l'administration de la justice et la sécurité publique, les décisions administratives ou politiques et la vérification.

6.3. Responsabilité et imputabilité

L'efficacité de la sécurité de l'information exige l'attribution claire des responsabilités à tous les niveaux de l'organisation, y compris les partenaires et les fournisseurs du Ministère. Elle nécessite en outre la mise en place d'un processus de gestion interne de la sécurité de l'information permettant une reddition de comptes adéquate.

6.4. Conformité aux lois, règlements et normes applicables

En plus du cadre de gestion gouvernemental de la sécurité de l'information et ses documents afférents, le Ministère doit se conformer aux lois, règlements et normes applicables.

Ainsi, tout utilisateur doit se conformer aux exigences relatives à l'utilisation de produits, documents et information, à l'égard desquels il pourrait y avoir un droit de propriété intellectuelle. Ainsi, l'utilisation des logiciels propriétaires et des logiciels libres doit respecter la Loi sur le droit d'auteur (L.R.C. 1985, c. C-42). Le Ministère doit ainsi assurer une gestion adéquate des licences de ses logiciels et, à cet effet, maintenir un inventaire de ceux-ci en conformité avec cette loi.

Seuls les logiciels fournis par le Ministère doivent être utilisés. L'utilisation de tout autre logiciel doit obligatoirement faire l'objet d'une autorisation spécifique du responsable organisationnel de la sécurité de l'information (ROSI).

Le Ministère peut choisir de se conformer à différentes normes et à divers standards en sécurité de l'information (ex. : normes ISO). En outre, le Ministère a l'obligation de s'assurer qu'il répond aux exigences relatives à la norme PCI-DSS[3].

6.5. Évolution

Les pratiques et les solutions du Ministère en matière de sécurité de l'information doivent être réévaluées périodiquement afin de tenir compte des changements juridiques, organisationnels, humains et technologiques ainsi que de l'évolution des menaces et des risques.

[3] *Payment Card Industry – Data Security Standard*

6.6. Universalité

Les pratiques et les solutions du Ministère en matière de sécurité de l'information doivent correspondre, dans la mesure du possible, à des façons de faire reconnues et généralement utilisées au gouvernement du Québec ainsi qu'à l'échelle nationale et internationale.

6.7. Éthique

Le processus de gestion de la sécurité de l'information doit être soutenu par une démarche éthique visant notamment la responsabilisation collective et individuelle.

6.8. Séparation des tâches incompatibles

La séparation des tâches incompatibles est un concept bien établi en matière de contrôle de vérification. Elle consiste à 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 toute personne concernée dans une situation où celle-ci pourrait les dissimuler.

6.9. Sensibilisation et formation

Le Ministère s'engage, sur une base régulière, à sensibiliser et à former les utilisateurs à la sécurité des actifs informationnels, aux conséquences d'une atteinte à la sécurité de ces actifs ainsi qu'à leur rôle et leurs obligations en la matière.

Par ailleurs, le Ministère favorise le recours aux services communs de formation en sécurité de l'information donnés par le Centre de services partagés du Québec (CSPQ) par l'intermédiaire de son Centre de leadership et de développement des compétences (CLDC).

6.10. Signalement des incidents liés à la sécurité

Le Ministère doit disposer d'un processus de gestion des incidents.

Tout utilisateur a l'obligation de signaler, sans tarder, à son gestionnaire ou au service de soutien aux utilisateurs, tout acte susceptible de représenter une atteinte réelle ou présumée à la sécurité de l'information.

Le responsable organisationnel de la sécurité de l'information (ROSI) doit également être avisé lorsque survient un incident de sécurité, afin de convenir des mesures à mettre en œuvre pour résoudre le problème, le cas échéant.

Les incidents doivent être répertoriés dans un registre des incidents et être analysés et classifiés selon leur gravité.

7. Orientations stratégiques

Les orientations stratégiques en matière de sécurité de l'information s'appuient sur les principes directeurs. Elles constituent le fondement des processus, directives, procédures, pratiques et autres mesures de sécurité nécessaires pour assurer la protection de l'information et des actifs informationnels.

7.1. Cohérence de la sécurité de l'information

L'information détenue, traitée ou utilisée par le Ministère est essentielle à sa mission et à ses opérations courantes et doit faire l'objet d'une utilisation et d'une protection adéquates durant tout son cycle de vie. La sécurité de l'information doit reposer sur une approche globale et intégrée qui tient compte des aspects juridiques, humains, éthiques, organisationnels et technologiques. Cette approche nécessite la mise en œuvre d'un ensemble de mesures cohérentes et coordonnées de prévention, de dissuasion, de détection, de signalement, de correction et de sanction.

En ce sens, le Ministère s'engage formellement à soutenir toutes les mesures qui s'inscrivent dans le cadre de cette politique de sécurité de l'information. Il s'engage également à mettre de l'avant les moyens nécessaires à leur réalisation afin de minimiser les risques et d'assurer une gestion saine et intégrée de la sécurité de l'information au sein de l'organisation.

7.2. Responsabilité collective et individuelle

Cette politique s'inscrit dans une perspective proactive. L'atteinte d'un degré optimal en sécurité de l'information nécessite l'adhésion de tous à une vision et à une compréhension communes de la sécurité de l'information et doit s'appuyer sur l'engagement continu du Ministère et des utilisateurs. La responsabilité en matière de sécurité de l'information repose donc sur un engagement collectif et individuel à :

- protéger l'information qui est mise à sa disposition en l'utilisant avec discernement et aux seules fins prévues ;
- protéger l'ensemble des moyens, biens et lieux qui permettent d'avoir accès à cette information.

Un registre d'autorité ministériel doit être tenu à jour afin d'y consigner la désignation des détenteurs de l'information jugée stratégique et de partager clairement les responsabilités en matière de sécurité de l'information à tous les niveaux de l'organisation. Ce registre,

approuvé par le sous-ministre, soutient le processus de gestion interne de la sécurité permettant une reddition de comptes adéquate.

7.3. Sécurité dans les contrats et les ententes

Des dispositions garantissant le respect des exigences en matière de sécurité de l'information sont intégrées aux contrats et aux ententes de service. Toute ressource externe ayant accès à de l'information confidentielle ou à des renseignements personnels doit respecter un engagement de confidentialité dont elle prend connaissance avant le début du mandat. Tout prestataire de services a l'obligation de s'assurer que ses employés respectent cette politique.

Le Ministère prévoit des sanctions en cas de manquement majeur de son application.

7.4. Gestion des risques

Le choix des mesures de sécurité s'appuie sur la détermination et l'évaluation périodiques des risques qui menacent l'information et les actifs informationnels. Ce choix tient compte des risques résiduels acceptables, des enjeux que ceux-ci comportent pour le Ministère et pour le gouvernement, ainsi que des coûts associés à l'implantation des mesures établies.

Une évaluation des risques est réalisée dès le début des études menant à la conception ou à l'acquisition d'un système d'information ou à tout changement important pouvant l'affecter, ou toucher l'infrastructure technologique ou la prestation des services et la sécurité de l'information.

7.5. Continuité des services

Le Ministère doit disposer d'un processus de gestion de la continuité des services, comprenant un plan de reprise informatique, qui permet de parer à des cas de sinistre ou d'incident majeur[4] touchant la disponibilité de l'information afin de permettre, dans un délai raisonnable, le rétablissement des processus d'affaires et des systèmes d'information jugés essentiels.

Un plan de sauvegarde de l'information électronique ministérielle doit être établi et révisé périodiquement. Ce plan précise, entre autres, la fréquence des copies de sauvegarde, le calendrier de rotation des médias, le lieu d'entreposage de ces médias ainsi que les personnes responsables des activités de mise en œuvre.

[4] Un sinistre ou un incident majeur peuvent être, par exemple, un incendie, une attaque cybernétique ou une panne de courant prolongée.

Un sous-comité sur la continuité des services est également mis en place par le sous-ministre afin, notamment, d'assurer une gestion coordonnée des mesures ministérielles et des liens avec les intervenants de l'extérieur du Ministère, le cas échéant.

8. Principaux rôles et responsabilités

Cette section présente les rôles et responsabilités des principaux intervenants en matière de sécurité de l'information au Ministère. L'ensemble des rôles détaillés et des structures internes de coordination est décrit dans le Cadre de gestion de la sécurité de l'information.

8.1. Sous-ministre

Le sous-ministre est le premier responsable de la sécurité de l'information relevant de son autorité. Il doit assurer le respect des lois et des règles de sécurité de l'information déterminées par le Secrétariat du Conseil du trésor, notamment en ce qui a trait à la mise en place de mesures permettant la réduction des risques de sécurité de l'information. À ce titre, il doit, notamment :

- s'assurer de la mise en place de mesures permettant de réduire les risques de sécurité de l'information à un niveau acceptable pour l'organisation;
- s'assurer de l'adéquation des mesures de sécurité de l'information en vigueur par rapport aux risques encourus;
- désigner les principaux intervenants en sécurité de l'information, dont les détenteurs de l'information.

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

Le sous-ministre désigne le responsable organisationnel de la sécurité de l'information (ROSI). Le ROSI joue le rôle de porte-parole du dirigeant principal de l'information et relaie les orientations et les priorités d'intervention gouvernementales en sécurité de l'information. Il assure la coordination et la cohérence des mesures de sécurité de l'information mises en œuvre par d'autres intervenants du Ministère. Il coordonne également la contribution du Ministère aux processus de gestion des risques et de gestion des incidents à portée gouvernementale.

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

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

8.4. Coordonnateur organisationnel en gestion des incidents (COGI)

Le coordonnateur organisationnel de la gestion des incidents (COGI) est désigné par le sous-ministre et collabore étroitement avec le ROSI et le COSI afin de leur fournir le soutien technique nécessaire à l'exercice de leurs responsabilités. Il participe activement au réseau d'alertes gouvernemental et contribue à la mise en place du processus de gestion des incidents au sein de son organisation et du processus de gestion des incidents à portée gouvernementale.

8.5. Détenteur de l'information

Toute personne qui est désignée par le sous-ministre et dont le rôle est, notamment, de s'assurer de la sécurité de l'information et des ressources qui la sous-tendent relevant de la responsabilité de son unité administrative. Le terme « détenteur de processus d'affaires » est utilisé lorsque ce rôle se limite à un processus d'affaires déterminé.

8.6. Utilisateur

Toute personne visée par la politique, telle qu'elle est définie à la section 5.2, a l'obligation de la respecter afin de protéger convenablement l'information mise à sa disposition.

9. Comités ministériels

Le Cadre de gestion de la sécurité de l'information du Ministère explique aussi les rôles et responsabilités des comités ministériels en matière de sécurité de l'information :

- Comité chargé de la sécurité de l'information;
  - Sous-comité de gestion des incidents et de continuité des services;
  - Sous-comité de l'accès à l'information et de la protection des renseignements personnels.

10. Dispositions finales

Le Ministère peut adopter des directives et des procédures de sécurité afin de soutenir et de préciser l'application de cette politique en vue, notamment, d'assurer la sécurité de l'information dans des domaines d'application particuliers.

10.1. Mesures d'exception

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

10.2. Droit de regard

Le Ministère a droit de regard sur la manipulation et l'utilisation de ses données par les utilisateurs. Ce droit s'exerce en conformité avec les lois et les règlements et s'étend non seulement aux opérations effectuées à partir des équipements normalisés du Ministère, mais également de tout autre équipement, personnel ou professionnel, susceptible de saisir ou de reproduire l'information du Ministère ou d'y accéder.

10.3. Mesures disciplinaires

Lorsqu'un utilisateur contrevient à cette politique ou à tout autre document directif qui en découle, des mesures disciplinaires ou administratives peuvent être appliquées en fonction de la gravité de son geste. Ces mesures peuvent inclure la suspension des privilèges, l'avertissement, la réprimande, la suspension, le congédiement, ou toutes autres mesures appropriées.

Le Ministère peut aussi transmettre à toute autre autorité judiciaire les renseignements colligés et qui le portent à croire qu'une infraction à toute loi ou à tout règlement en vigueur a été commise.

10.4. Mise en œuvre, suivi et révision

Le responsable organisationnel de la sécurité de l'information (ROSI) s'assure de la mise à jour et de la mise en œuvre des dispositions de cette politique et de ses directives d'application.

Cette politique doit être révisée à l'occasion de changements qui pourraient la toucher ou, au plus tard, tous les trois ans à partir de sa date d'approbation. Toute modification devra

être approuvée par le sous-ministre, sur recommandation du Comité chargé de la sécurité de l'information.

10.5. Approbation et date d'entrée en vigueur

Cette politique remplace la Politique concernant la sécurité de l'information approuvée le 5 novembre 2008. Elle entre en vigueur à la date d'approbation.

Original signé 10 mai 2015

_____ _____

M. Gilbert Charland Date

Sous-ministre

ANNEXE I – DÉFINITIONS

Actif informationnel
Une information, quels que soient son canal de communication (téléphone analogique ou numérique, télégraphe, télécopie, voix, etc.) ou son support (papier, pellicule photographique ou cinématographique, ruban magnétique, support électronique, etc.), un système ou un support d'information, une technologie de l'information, une installation ou un ensemble de ces éléments, acquis ou constitués par une organisation.

Confidentialité
Propriété qu'ont les données ou l'information de n'être accessibles qu'aux personnes autorisées à en prendre connaissance.

Continuité des services
Capacité d'une organisation d'assurer, en cas de sinistre, la poursuite de ses processus d'affaires selon un niveau de service prédéfini.

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 du Ministère.

Disponibilité
Propriété d'une information d'être accessible en temps voulu et de la manière requise pour une personne autorisée.

Document
Ensemble constitué d'information portée par un support. L'information y est délimitée, 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 transcriptibles sous l'une de ces 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.
[Source : Loi concernant le cadre juridique des technologies de l'information - article 3]

Gestion des risques en sécurité de l'information
Processus de détermination, de contrôle et de réduction des risques de sécurité qui pourraient nuire à l'information.

Guide
Document administratif à caractère pédagogique qui vise à faciliter l'application des prescriptions d'une politique, d'une directive ou éventuellement d'une norme, sans en avoir le caractère contraignant. [Source : Grand dictionnaire terminologique]

Incident
Événement qui ne fait pas partie du fonctionnement normal d'un service, quel que soit son mode de prestation, et qui entraîne, ou peut entraîner, une interruption ou une détérioration de la qualité de ce service.

Incident de sécurité de l'information à portée gouvernementale
Conséquence observable de la concrétisation d'un risque de sécurité de l'information à portée gouvernementale et qui nécessite une intervention concertée sur le plan gouvernemental.

Information
Renseignements consignés sur un support quelconque, dans un but de transmission des connaissances.

Intégrité
Propriété d'une information de ne subir aucune altération ou destruction de façon erronée ou sans autorisation et d'être conservée sur un support lui procurant stabilité et pérennité. L'intégrité fait référence à l'exactitude et à la complétude.

Mesure de sécurité de l'information
Moyen concret assurant, partiellement ou totalement, la protection d'un actif informationnel contre un ou plusieurs risques et dont la mise en œuvre vise à amoindrir la probabilité de survenance de ces risques ou à réduire les pertes qui en résultent.
[Source : OQLF – Grand dictionnaire terminologique]

Norme
Accord entériné par un organisme officiel de normalisation comme l'Organisation internationale de normalisation (ISO), le Conseil canadien des normes (CCN), etc., contenant des spécifications techniques ou autres critères précis destinés à être utilisés systématiquement en tant que règles, lignes directrices ou définitions de caractéristiques pour assurer que des matériaux, produits, processus et services sont aptes à leur emploi.
[Source : Lexique gouvernemental]

Pratique
Savoir ou manière de faire qui, dans une organisation, conduisent au résultat souhaité et qui sont portés en exemple auprès des pairs afin de leur faire partager l'expérience qui leur permettra une amélioration collective.
[Source : Inspirée de l'OQLF – Grand dictionnaire terminologique]

Procédure
Ensemble des étapes à franchir, des moyens à prendre et des méthodes à suivre dans l'exécution d'une tâche.
[Source : OQLF – Grand dictionnaire terminologique]

Processus
Suite cohérente d'activités et d'opérations d'une organisation traduisant les besoins de la clientèle et des employés dans une logique de création de valeur.

Registre d'autorité
Répertoire, recueil ou fichier, dans lequel sont inscrites les désignations effectuées et les délégations consenties aux fins de la gestion de la sécurité, ainsi que les responsabilités qui y sont rattachées.

Registre d'incident
Recueil dans lequel sont consignés la nature de l'incident, l'impact, les mesures prises pour le rétablissement à la normale et le suivi.

Renseignement confidentiel
Tout renseignement dont l'accès est assorti d'une ou de plusieurs restrictions prévues par la Loi sur l'accès. Il peut avoir, par exemple, des incidences sur les relations intergouvernementales, les négociations entre organismes publics, l'économie, l'administration de la justice et de la sécurité publique, les décisions administratives ou politiques ou sur la vérification.

Renseignement personnel
Tout renseignement qui concerne une personne physique et permet de l'identifier. Un renseignement personnel qui a un caractère public en vertu d'une loi n'est pas considéré comme un renseignement personnel aux fins de la politique de sécurité.
[Source : *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*]

Sécurité physique
Mesures physiques prises pour assurer la protection des personnes et des biens, empêcher, notamment tout accès non autorisé aux équipements, installations et documents, et les protéger contre toute forme de menace physique ou accidentelle. La sécurité physique porte autant sur la salle des serveurs, son périmètre, les bâtiments et locaux tels que les bureaux, les salles informatiques, les locaux techniques, que sur les matériels de servitude, l'équipement informatique et les supports informatiques tels que les disques, les disquettes et les bandes magnétiques, sans oublier les listages et la documentation.

Standard
Norme qui n'a pas été définie ni entérinée par un organisme officiel de normalisation, comme l'Organisation internationale de normalisation (ISO), le Conseil canadien des normes (CCN), etc., mais qui s'est imposée par la force des choses, parce qu'elle fait consensus auprès des utilisateurs, d'un groupe d'entreprises ou encore d'un consortium.

ANNEXE II – CADRE LÉGAL ET ADMINISTRATIF

CANADA

- Charte canadienne des droits et libertés de la Loi constitutionnelle de 1982;
- Code criminel, L.R., 1985, c. C-46;
- Loi sur le droit d'auteur, L.R., 1985, c. C-42.

QUÉBEC

Lois et règlements

- Code civil du Québec;

- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, chapitre A-2.1 :
    - Règlement sur la diffusion de l'information et sur la protection des renseignements personnels, chapitre A-2.1, r. 2;

- Loi sur l'administration financière, chapitre A-6.001;

- Loi sur l'administration publique, chapitre A-6.01;

- Loi sur les archives, chapitre A-21.1;

- Loi concernant le cadre juridique des technologies de l'information, chapitre C-1.1;

- Charte des droits et libertés de la personne, chapitre C-12;

- Loi sur la fonction publique, chapitre F-3.1.1 :
    - Règlement sur l'éthique et la discipline dans la fonction publique, chapitre F-3.1.1, r. 3;

- Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, chapitre G-1.03;

- Loi sur la protection des renseignements personnels dans le secteur privé, chapitre P-39.1;

- Loi sur la sécurité civile, chapitre S-2.3.

Directives

- Directive sur la sécurité de l'information gouvernementale, Décret 7-2014 du 15 janvier 2014 :
    - Cadre gouvernemental de gestion de la sécurité de l'information;
    - Cadre de gestion des risques et des incidents à portée gouvernementale en matière de sécurité de l'information,

- Approche stratégique triennale 2014-2017 en sécurité de l'information gouvernementale.

- Directive sur les services de certification offerts par le gouvernement du Québec, Décret 6-2014 du 15 janvier 2014;

- Directive sur l'utilisation du courriel, d'un collecticiel et des services d'Internet par le personnel de la fonction publique, C.T. 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 sur un support informatique amovible C.T. 193953 du 19 octobre 1999, modifié par le C.T. 199891 du 27 mai 2003.