Politique de sécurité de l'information

Version 2.0
Approuvée le 7 juin 2021
Entrée en vigueur le 7 juin 2021
Révision prévue en juin 2026

MINISTÈRE DE L'ÉNERGIE ET DES RESSOURCES NATURELLES

MINISTÈRE DES FORÊTS, DE LA FAUNE ET DES PARCS

Votre gouvernement

Québec

Table des matières

Contexte

Le ministère de l'Énergie et des Ressources naturelles (MERN) 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 ». Le ministère des Forêts, de la Faune et des Parcs (MFFP) a pour mission « d'assurer une gestion durable des forêts, de la faune et des parcs et d'appuyer le développement économique de ces secteurs d'activité au bénéfice des citoyens du Québec et de ses régions ».

La sécurité de l'information repose sur trois aspects fondamentaux : la disponibilité, l'intégrité et la confidentialité. Ces aspects sont d'autant plus importants qu'ils sont à la base du respect de la vie privée et de la protection des renseignements personnels.

Le MERN a adopté en mai 2015 une Politique de sécurité de l'information (ci-après nommée « Politique » qui décrit un ensemble d'énoncés et principes, ainsi qu'un cadre de gestion que l'organisation doit respecter et mettre en œuvre. La Politique a été adoptée en application de la Directive sur la sécurité de l'information gouvernementale du Secrétariat du Conseil du trésor (SCT), qui confère aux organismes de nouvelles obligations en matière de sécurité de l'information.

La mise en œuvre de cette Politique a permis d'introduire une nouvelle culture de sécurité de l'information au sein du MERN et d'apporter une amélioration du niveau global de la sécurité.

Toutefois, le MERN a connu des changements organisationnels structurants résultant du décret 288-2016 du 13 avril 2016 de la *Loi sur le ministère des Ressources naturelles et de la Faune*. La mise en œuvre de projets, l'évolution des pratiques dans une perspective d'optimisation (amélioration continue), de partage des ressources entre le MERN et le MFFP et la modernisation des services ont engendré la nécessité de faire évoluer l'encadrement actuel de la sécurité de l'information par de nouvelles dispositions pour assurer la disponibilité, l'intégrité et la confidentialité de l'information.

En matière de sécurité de l'information, le MERN et le MFFP travaillent en étroite et constante collaboration. Ce dernier bénéficie de services partagés offerts par le MERN (ci-après nommé « le Ministère ») en ce qui concerne la gestion des ressources humaines, financières, matérielles et contractuelles. Enfin, le MERN et le MFFP (ci-après nommées « les organisations ») ont le même dirigeant de l'information pour les représenter auprès du dirigeant principal de l'information du SCT.

Compte tenu de sa nature hautement sensible, la sécurité de l'information revêt une importance capitale pour les organisations 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 constitue la pierre d'assise de la gouvernance des organisations en la matière et incarne leurs visions respectives. Elle décrit les objectifs, le champ d'application, les principes directeurs, ainsi que les rôles et les responsabilités des principaux acteurs. La présente Politique assure aussi le respect des obligations qui sont établies en vertu de la *Directive sur la sécurité de l'information gouvernementale*. Sa mise en œuvre est notamment soutenue par un cadre de gestion de la sécurité de l'information.

Définitions

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

Cadre légal et administratif

Les organisations doivent respecter un cadre normatif s'appliquant à l'information et aux documents qu'elles détiennent. Plusieurs lois et règlements encadrent la sécurité de l'information ainsi que l'accès et la protection des renseignements personnels. 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) 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 SCT, 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.

La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels* assurent une protection maximale des renseignements personnels que détiennent les organisations en permettant à quiconque qui en fait la demande, l'accès aux documents des organismes publics à l'intérieur des délais établis par cette loi, sous réserve de certaines restrictions.

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

Objectifs de la Politique

La Politique de sécurité de l'information a pour objectif d'affirmer l'engagement des organisations de s'acquitter pleinement de leurs obligations à l'égard de la sécurité de l'information, quel que soit le support ou le moyen de communication utilisé et quel que soit l'utilisateur. Plus précisément, elle a pour but :

- d'atteindre un degré adéquat et une compréhension commune de la sécurité de l'information et l'engagement constant de tous les utilisateurs des organisations ainsi que de ses partenaires, fournisseurs, prestataire de services et clients;
- de s'assurer que le personnel et les parties prenantes sont conscients et tenus informés de leurs responsabilités en matière de sécurité de l'information;
- de développer une culture d'entreprise pour s'assurer que le personnel et l'administration prennent en compte la sécurité de l'information dans leur activité quotidienne;
- d'assurer un niveau de disponibilité, de confidentialité et d'intégrité nécessaire à la protection de l'information durant tout son cycle de vie;
- d'assurer une gestion saine des identités et des accès aux ressources des organisations;
- d'assurer le respect de la conformité aux différents cadres légaux, administratifs et normatifs auxquels sont assujetties les organisations.

Champ d'application

Cette Politique relative à l'accès, la protection et la sécurité de l'information porte sur l'information détenue ou utilisée par les organisations, peu importe la nature de l'information, sa localisation ou son support, et ce, durant tout son cycle de vie. Elle couvre ainsi les domaines organisationnels, technologiques, physiques et environnementaux, la gestion documentaire et la gestion contractuelle.

INFORMATION ET ACTIFS INFORMATIONNELS VISÉS

La Politique de sécurité de l'information s'applique de façon non restrictive aux catégories d'information suivantes :

- l'information appartenant aux organisations et exploitée par celles-ci;
- l'information appartenant aux organisations et exploitée ou détenue par un partenaire, un fournisseur de produits, un prestataire de services ou un autre intervenant;
- l'information appartenant à un partenaire, à un fournisseur de produits, un prestataire de services, ou un autre intervenant, et exploitée par lui au profit des organisations.

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

PERSONNES VISÉES

Cette Politique s'adresse aux utilisateurs, c'est-à-dire toute personne physique ou morale ayant accès à l'information et aux actifs informationnels des organisations sans égard au statut d'emploi, y compris les employés permanents ou occasionnels et les personnes en prêts de service, les étudiants et les stagiaires ainsi qu'à tous les partenaires, les fournisseurs, les prestataires de services, les clients ou autres intervenants.

ACTIVITÉS VISÉES

Toute activité impliquant la création, l'utilisation, le traitement, la communication ou la conservation d'une information ou d'un actif informationnel appartenant aux organisations est visée par la présente Politique, qu'elle soit conduite dans ses locaux, dans un autre lieu ou à distance. Il s'agit notamment d'activités liées à :

- la constitution de l'information ou d'un actif informationnel;
- le développement de projet;
- l'exploitation et l'administration des infrastructures des technologies de l'information;
- la gestion des actifs ou du semi-actif informationnels et leur versement aux archives ou destruction;
- la gestion des télécommunications;
- la gestion des édifices et des locaux des organisations.

Principes directeurs

La sécurité de l'information a pour but de maintenir, voire rehausser, la confiance de la population à l'égard de l'État et des services qu'il fournit et de contribuer à la réalisation de sa mission et de celle des organisations. Elle a également pour but d'assurer la pérennité d'une information fiable. Une démarche éthique, visant notamment la responsabilisation collective et individuelle, soutient le processus de gestion de la sécurité de l'information. Les pratiques et les solutions retenues en matière de sécurité de l'information doivent être exemplaires, tenir compte des bonnes pratiques reconnues et généralement utilisées à l'échelle nationale et internationale.

Les organisations assurent la sécurité de l'information et la protection des renseignements personnels conformément aux principes directeurs suivants.

APPROCHE GLOBALE DE LA SÉCURITÉ DE L'INFORMATION

La gestion de la sécurité de l'information repose sur une approche globale qui tient compte des aspects financiers, organisationnels, humains, juridiques et technologiques. Elle exige la mise en place d'un ensemble de mesures de sécurité coordonnées, cohérentes, adaptées aux missions des deux ministères et supportant les besoins d'affaires.

PROTECTION DE L'INFORMATION

Les organisations adhèrent aux orientations et objectifs stratégiques gouvernementaux en matière de sécurité de l'information et s'engagent à ce que les pratiques et les solutions retenues en la matière correspondent, dans la mesure du possible, à des façons de faire en respect du principe d'universalité. L'information détenue est essentielle à sa mission et doit faire l'objet d'une évaluation constante ainsi que d'une utilisation et d'une protection adéquate durant tout son cycle de vie. Le niveau de protection accordé est établi en fonction du degré de sensibilité de l'information.

Tout renseignement considéré comme personnel ou confidentiel doit être protégé contre tout accès ou utilisation non autorisée ou illicite, et ce, en vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*.

DISPONIBILITÉ DE L'INFORMATION

L'information doit être accessible en temps voulu et de la manière requise par un utilisateur autorisé. L'accessibilité de l'information présente dans les documents technologiques est assurée pendant toute leur période de conservation. L'archivage ou la destruction des documents qui ne sont plus nécessaires est réalisé selon la classification de l'information et le calendrier de conservation des documents.

INTÉGRITÉ DE L'INFORMATION

Le support de l'information lui procure la stabilité et la pérennité voulues, et cette information ne doit pas être altérée ou détruite sans autorisation ou en contradiction au calendrier de conservation. Des mesures de sécurité physiques et d'accès logiques protègent l'information contre la perte ou le dommage accidentel ou délibéré. L'intégrité des documents est assurée tout au long de leur cycle de vie de manière à préserver leur valeur.

CONFIDENTIALITÉ DE L'INFORMATION

L'information, surtout si elle est constituée de renseignements personnels, doit être accessible ou divulguée qu'aux personnes ou entités désignées et autorisées. La confidentialité de l'information est assurée tout au long de son cycle de vie par, en autre, une gestion éprouvée des identités et des accès.

RESPONSABILITÉ ET IMPUTABILITÉ

La sécurité de l'information représente une responsabilité collective où chaque personne est imputable de l'utilisation qu'elle fait de l'information dont elle a été dûment autorisée à avoir accès. À cette fin, le membre du personnel répond de ses actions auprès du plus haut dirigeant.

L'efficacité de la sécurité de l'information exige l'attribution claire des responsabilités à tous les niveaux de l'organisation, y compris auprès des partenaires et des fournisseurs ou prestataires de services, et de la mise en place d'un processus de gestion interne de la sécurité permettant une reddition de comptes adéquate. Tous les utilisateurs ont l'obligation de signaler aux autorités compétentes de leur ministère, tout acte représentant une violation réelle ou présumée des règles de sécurité comme le vol, l'intrusion, l'utilisation abusive, la fraude, etc.

RESPECT DU DROIT D'AUTEUR

Les utilisateurs des organisations doivent se conformer aux exigences légales portant sur l'utilisation des produits à l'égard desquels il y a des droits de propriété intellectuelle et sur l'utilisation de produits logiciels propriétaires.

GESTION INTÉGRÉE DU RISQUE ET CATÉGORISATION DE L'INFORMATION

La mise en œuvre d'une gouvernance forte et intégrée de la sécurité de l'information dans les organisations nécessite la mise en place d'un processus de gestion des risques basé sur l'amélioration continue permettant l'identification, l'analyse et le traitement des risques de sécurité et des risques à portée gouvernementale à tous les niveaux hiérarchiques de l'organisation.

Sur une base récurrente, une analyse de risques est effectuée pour chaque domaine d'activité visé par la présente Politique afin d'identifier les risques pouvant affecter la réalisation de leur mission. L'information est catégorisée par leur détenteur dès l'étape de la conception d'un système d'information. Elle est protégée selon le besoin en matière de disponibilité, d'intégrité et de confidentialité de façon à considérer les mesures applicables en sécurité de l'information. Le choix des mesures de protection s'appuie sur une analyse des risques auxquels l'information peut être exposée.

GESTION DES INCIDENTS

La prise en charge de manière efficace et efficiente des incidents de sécurité et des incidents majeurs repose sur un processus de gestion des incidents précisant les actions à entreprendre et les rôles et responsabilités de chaque acteur. Ce processus inclut la gestion des incidents à portée gouvernementale qui nécessite une coordination ministérielle et gouvernementale.

GESTION DES IDENTITÉS ET DES ACCÈS

L'accès aux ressources informationnelles requiert des mesures de contrôles d'accès logiques éprouvées et respectant les standards et meilleures pratiques en matière de gestion des identités et des accès. L'accès à l'information est autorisé uniquement aux ressources dont les tâches le requièrent en respectant le principe du moindre privilège afin de s'assurer que l'utilisateur ne dispose pas de plus de droits que nécessaire à accomplir ses tâches. Il est soutenu par un processus qui prend en compte les risques de sécurité auxquels les organisations peuvent être exposées. Les meilleures pratiques en matière de journalisation des accès sont mises en place afin de permettre la vérification de la conformité des accès à l'information.

GESTION DE LA SÉCURITÉ PHYSIQUE

La sécurité physique concerne la protection de l'accès physique aux locaux des organisations, des équipements, des documents et des personnes. Elle vise, en autre, à empêcher tout accès physique non autorisé, ainsi que tout dommage ou intrusion portant sur l'information ou sur les locaux qui abritent des systèmes et des installations technologiques stratégiques. Elle touche également la mise au rebut sécuritaire des supports de l'information.

GESTION DE LA REPRISE ET DE LA CONTINUITÉ DES AFFAIRES

Les applications, les services ainsi que les infrastructures essentielles des organisations bénéficient de solutions adéquates de reprise et de continuité des affaires. Ces solutions sont déterminées pour répondre à différents types de risques et d'événements, chacun étant caractérisé par leurs niveaux de sévérité et d'impacts sur les pratiques d'affaires. Le fonctionnement des solutions de reprise est validé, testé et, si requis, corrigé selon le processus en vigueur.

GESTION DES CONTRACTANTS ET DES CONTRATS

Les organisations doivent utiliser un processus de gestion de leurs fournisseurs ou prestataires de services afin de s'assurer de l'intégration de dispositions dans les ententes et les contrats de service qui garantissent le respect des exigences en matière de sécurité de l'information. Ce processus tient compte des risques spécifiques de l'infonuagique.

GESTION DES VULNÉRABILITÉS

Les organisations déploient des mesures pour maintenir à jour les logiciels du parc informatique afin de garder les vulnérabilités au niveau le plus bas possible et diminuer les chances d'une cyberattaque. Une gestion de notification des vulnérabilités venant des fournisseurs ou des prestataires de services doit être en place pour qu'elles soient évaluées et corrigées le cas échéant.

SENSIBILISATION ET FORMATION

Les organisations s'engagent 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. L'utilisateur a la responsabilité de participer à ces activités de sensibilisation et de formation. Par ailleurs, les organisations favorisent le recours aux services communs de formation en sécurité de l'information.

VÉRIFICATION

Des vérifications périodiques sont effectuées pour évaluer la performance des mesures de sécurité mises en œuvre pour une assurance de la protection de l'information des organisations. Elles sont soutenues par un processus rigoureux et effectué par des personnes dûment habilitées et ciblent aussi toute activité contrevenant aux cadres légaux, réglementaires et administratifs.

ÉVOLUTION

Les pratiques et les solutions des organisations 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.

Principaux rôles et responsabilités

L'ensemble des rôles et responsabilités, et les structures internes de coordination sont décrits dans le Cadre de gestion de la sécurité de l'information.

Le dirigeant de l'information (DI) désigné par le ministre veille à la mise en œuvre et au suivi des recommandations émises par le Conseil du trésor ou par le dirigeant principal de l'information (DPI).

Le Responsable organisationnel de la sécurité de l'information (ROSI) assure la coordination et la cohérence des actions, dont les principales portent sur l'adoption de la présente Politique et d'un cadre de gestion de la sécurité de l'information ainsi que sur la mise en œuvre de processus officiels de gestion des risques, de gestion de l'accès à l'information et de gestion des incidents de sécurité de l'information.

Les sous-ministres du MERN et du MFFP, en tant que premiers responsables de la sécurité de l'information, approuvent conjointement la présente Politique et s'assurent entre autres du respect des lois et règles de sécurité du gouvernement ainsi que de celles spécifiquement applicables à leur organisation.

La Direction générale des ressources informationnelles (DGRI) par l'entremise de la Direction de l'amélioration continue et de l'innovation numérique (DACIN), est responsable de l'élaboration et de l'application de la présente Politique.

Tous les gestionnaires des organisations sont responsables du respect de la présente Politique au sein de leurs unités administratives respectives.

Tous les utilisateurs des organisations doivent y adhérer et s'y conformer. Chaque utilisateur a comme principale obligation de protéger l'information mise à sa disposition.

Le Comité chargé de la sécurité de l'information est la principale instance de concertation en matière de sécurité de l'information. Il coordonne les différentes activités relatives à la sécurité de l'information.

Dispositions finales

Les organisations peuvent 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.

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 du Ministère.

DROIT DE REGARD

Les organisations ont droit de regard sur l'utilisation de leurs données. 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, accéder, conserver ou de reproduire l'information du Ministère.

MESURES DISCIPLINAIRES

Lorsqu'un utilisateur contrevient à cette Politique ou à toute directive y découlant, des mesures disciplinaires, administratives ou légales peuvent être appliquées en fonction de la gravité de son action.

MISE EN ŒUVRE, SUIVI ET RÉVISION

Le ROSI des organisations 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 tous les cinq ans à partir de sa date d'approbation à moins que des changements majeurs exigent de la réviser ponctuellement. Toute modification devra être approuvée par les sous-ministres, sur recommandation du Comité chargé de la sécurité de l'information mis en place conformément au Cadre de gestion de la sécurité de l'information.

APPROBATION ET DATE D'ENTRÉE EN VIGUEUR

Cette Politique de sécurité de l'information remplace la Politique de sécurité de l'information approuvée en mai 2015. Elle entre en vigueur à la date d'approbation.

Original signé *7 juin 2021*

_____ _____

Sous-ministre MERN Date

Original signé *7 juin 2021*

_____ _____

Sous-ministre MFFP Date

Annexe I - Définitions

Actif informationnel
Une information, quel que soit 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 affaires
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 son versement aux archives ou sa destruction, en conformité avec le calendrier de conservation.

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

Document
Un document est 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 réinscriptibles sous l'une de ces formes ou en un autre système de symboles.

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.

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 associée aux données qui, lors de leur traitement ou de leur transmission, ne subissent aucune altération ou destruction volontaire ou accidentelle, et conservent un format permettant leur utilisation.

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.

Pratique
Savoir ou manière de faire qui, dans une organisation, conduit 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.

Procédure
Ensemble des étapes à franchir, des moyens à prendre et des méthodes à suivre dans l'exécution d'une tâche.

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 valeurs.

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.

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 de l'information.

Reprise
Rétablissement d'une production informatique interrompue, détériorée ou détruite pour quelque cause que ce soit.

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.

Sources :

- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels;*
- *Loi concernant le cadre juridique des technologies de l'information - article 3;*
- *Directive sur la sécurité de l'information gouvernementale;*
- *Guide d'élaboration d'une politique de sécurité de l'information, SCT;*
- *Guide de catégorisation de l'information*, SCT;
- *OQLF – Grand dictionnaire terminologique.*

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

- Loi sur le ministère des Ressources naturelles et de la Faune;
- Code civil du Québec;
- Charte des droits et libertés de la personne, chapitre C-12;
- 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;
    - Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques, chapitre A-21.1, r. 2
- Loi concernant le cadre juridique des technologies de l'information, chapitre C-1.1;
- 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 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.

- 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;

- 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;

Énergie et Ressources naturelles
Québec