Politique ministérielle

Sécurité de l'information

Ministère de la Sécurité publique

Version : 1.2

Mise à jour : 2013-11-25

Québec

HISTORIQUE DES CHANGEMENTS

Version	Date	Description	Auteur
1.0	2009-06-01	Version officielle sur Intranet	ESGI
1.1	2012-10-12	Des modifications majeures sont apportées et plusieurs sections sont ajoutées	Samuel Morin – SSP
1.2	2013-11-25	Révision avant approbation	Samuel Morin, Claude Crête – SSP

Note : le masculin est utilisé pour alléger le texte. Les propos concernent autant les femmes que les hommes.

TABLE DES MATIÈRES

1. PRÉAMBULE

La présente politique est adoptée en application du paragraphe (a) du premier alinéa de l'article 7 de la Directive sur la sécurité de l'information gouvernementale. Celle-ci fait obligation aux organismes publics d'adopter et de mettre en œuvre une politique de sécurité de l'information, de la maintenir à jour et d'en assurer l'application.

2. DÉFINITION DE LA SÉCURITÉ DE L'INFORMATION

La sécurité de l'information 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 l'irrévocabilité des actions qu'ils posent.

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

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.

Confidentialité : Propriété d'une information de n'être accessible, ni divulguée qu'aux personnes ou entités désignées et autorisées.

Authentification : Propriété de permettre de confirmer l'identité d'une personne ou l'identification d'un document ou d'un dispositif;

Irrévocabilité : Qui est le fait pour une action ou un document d'être irréfutable et de pouvoir être clairement attribué à son auteur ou au dispositif qui l'a généré.

Cette définition implique que la sécurité de l'information 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 sécurité de l'information 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 l'éthique.

3. OBJECTIFS

La présente politique a pour objectif d'affirmer l'engagement du ministère à 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, il s'agit d'assurer, tout au long du cycle de vie de l'information, sa disponibilité, son intégrité et sa confidentialité.

4. CHAMP D'APPLICATION

La présente politique s'adresse aux utilisateurs, c'est-à-dire à tout le personnel peu importe son statut, à toute personne physique ou morale qui, à titre d'employé, de consultant, de partenaire ou de fournisseur, utilise les actifs informationnels du ministère ou y a accès ainsi qu'à toute personne dûment autorisée à y avoir accès.

L'information visée est celle que le ministère détient dans l'exercice de ses fonctions, que sa conservation soit assurée par lui-même ou par un tiers.

Cependant, les employés de la Direction générale de la Sûreté du Québec et de l'école nationale de police du Québec ne sont pas visés par cette politique.

5. ÉNONCÉS DE SÉCURITÉ

Les énoncés suivants constituent les orientations stratégiques et la vision d'encadrement de la sécurité de l'information que se donne le ministère de la Sécurité publique.

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

Le ministère adhère aux orientations et objectifs stratégiques gouvernementaux en matière de sécurité de l'information et s'engage à ce que les pratiques et les solutions retenues en la matière correspondent, dans la mesure du possible, à des façons de faire reconnu et généralement utilisé à l'échelle nationale et internationale.

Le ministère reconnaît que les actifs informationnels qu'il détient sont essentiels à ses activités courantes et, de ce fait, doivent faire l'objet d'une évaluation constante, d'une utilisation appropriée et d'une protection adéquate. Le niveau de protection dont les actifs informationnels doivent faire l'objet est établi en fonction de leur importance, de leur confidentialité et des risques d'accident, d'erreur et de malveillance auxquels ils sont exposés.

La sécurité des actifs informationnels est soutenue par une démarche d'éthique visant à assurer la régulation des conduites et la responsabilisation individuelle.

5.2. Protection des renseignements confidentiels

Toute information confidentielle doit être préservée de toute divulgation, de tout accès ou de toute utilisation non autorisée.

Sont notamment confidentiels les renseignements personnels 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.-21) ainsi que tout renseignement dont la divulgation aurait des incidences néfastes, notamment sur les relations 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.

5.3. Formation et sensibilisation

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 leur sécurité ainsi qu'à leur rôle et leurs obligations en cette matière.

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

Le ministère de la Sécurité publique doit maintenir l'intégrité de tout document ayant une valeur juridique nonobstant l'interchangeabilité de son 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.

5.5. Gérer la disponibilité et assurer la continuité des activités

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

Le ministère doit prévoir des mesures d'urgence, éprouvées et consignées par écrit, en vue d'assurer la remise en opération (dans un délai raisonnable) des systèmes d'information jugés essentiels en cas de sinistre majeur (ex. : incendie, attaque cybernétique, panne électrique prolongée, inondation, malveillance, etc.), et ce, dans le respect de ses obligations relatives à la Loi sur la sécurité civile.

5.6. Assurer la conservation des documents et leur disposition

Le ministère de la Sécurité publique est soumis aux politiques de gestion des documents actifs, semi-actifs et inactifs des organismes publics du gouvernement du Québec établis par Bibliothèque et Archives nationales du Québec. Dans ce contexte et pour assurer la conservation et la gestion intégrée des documents (GID), le ministère doit planifier et contrôler la création, l'utilisation, la conservation, et la disposition finales des documents, et ce, peu importe leur support.

La disposition des documents et des équipements déclarés en bien excédentaire ou confié à un fournisseur de services pour qu'il procède entre autres à leur entretien, à leur recyclage ou à leur destruction doit respecter la «*Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*» (L.R.Q.,c A-2.1, Art.63.1).

5.7. Évaluer et prendre en compte les risques en sécurité de l'information

Les risques et les menaces pour la sécurité de l'information doivent faire l'objet d'identification et d'évaluations périodique. Une évaluation des risques et le choix des mesures de sécurité doivent être effectués dès le début des études visant la conception, l'acquisition ou la mise en œuvre d'un changement important aux processus d'affaires, aux systèmes d'information, aux infrastructures ou aux supports de documents.

5.8. Exercer l'habilitation sécuritaire

La sécurité de l'information repose en premier lieu sur les employés du ministère de la Sécurité publique autorisés à exercer des fonctions au sein du ministère. Le ministère de la Sécurité publique affirme son droit de procéder à des vérifications et enquêtes de sécurité pour les personnes qui occupent des fonctions dans la gestion et l'utilisation de l'information.

5.9. Acquisition ou développement d'applications informatiques

Les exigences en matière de sécurité de l'information doivent être prises en considération dès le début des études 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.

5.10. Mesure 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.

6. RÔLE ET RESPONSABILITÉ DES INTERVENANTS PRINCIPAUX EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION

La présente politique fixe les obligations en matière de sécurité de l'information attribuées, notamment, au sous-ministre, au responsable organisationnel de sécurité de l'information, aux détenteurs, aux gestionnaires d'entités administratives et aux utilisateurs.

- Le sous-ministre : il est le premier responsable de la sécurité de l'information relevant de son autorité.
- Le dirigeant sectoriel de l'information (DSI) : il assure le suivi de la mise en œuvre des recommandations émises par le Conseil du trésor ou par le dirigeant principale de l'information.
- Le responsable organisationnel de la sécurité de l'information (ROSI) : il assiste le sous-ministre dans la détermination des orientations stratégiques et des priorités d'intervention.
- Le conseiller organisationnel en sécurité de l'information (COSI) : il élabore et met à jour la Politique ministérielle de sécurité de l'information, veille à la mise en application des normes de sécurité approuvées dans cette politique et élabore et assure le suivi et la mise à jour périodique du plan ministériel de sécurité de l'information.
- Le coordonnateur organisationnel de gestion des incidents (COGI) : il contribue aux analyses de risques de sécurité de l'information, identifie les menaces et les situations de vulnérabilité et met en œuvre les solutions appropriées. De plus, il contribue à la mise en place du processus de gestion des incidents de sécurité de l'information.
- Le détenteur de l'information : employé désigné par le ministère 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.

- Les gestionnaires : ils sont chargés de la mise en œuvre des dispositions de la présente politique auprès du personnel relevant de leur autorité.
- Les utilisateurs : ils doivent se conformer aux directives gouvernementales, à la présente politique et aux règles qui leur sont applicables en signant la déclaration d'engagement jointe à l'annexe.

Les rôles et les responsabilités attribués à d'autres intervenants ainsi que les structures internes de coordination et de concertation en matière de sécurité de l'information sont définies dans le cadre de gestion de la sécurité de l'information, en complément à la présente politique.

7. OBLIGATION DES UTILISATEURS

Tout utilisateur a l'obligation de protéger les actifs informationnels mis à sa disposition par le ministère. À cette fin, il doit :

- Prendre connaissance de la présente politique, des directives, des procédures et autres lignes de conduite en découlant, y adhérer et prendre l'engagement de s'y conformer en signant la déclaration jointe en annexe;
- Utiliser, à l'intérieur des droits d'accès qui lui sont attribués et uniquement lorsqu'ils sont nécessaires à l'exercice de ses fonctions, les actifs informationnels mis à sa disposition en se limitant aux fins auxquelles ils sont destinés;
- Respecter les mesures de sécurité mises en place sur son poste de travail et sur tout équipement contenant des données à protéger et ne pas modifier leur configuration ni les désactiver;
- Se conformer aux exigences légales sur l'utilisation de produits, documents et information à l'égard desquels il pourrait y avoir des droits de propriété intellectuelle.
- Signaler immédiatement à son supérieur tout acte, dont il a connaissance, susceptible de constituer une violation réelle ou présumée des règles de sécurité ainsi que toute anomalie pouvant nuire à la protection des actifs informationnels du ministère. Les incidents doivent être consignés dans un registre des évènements de sécurité.;
- Au moment de son départ du ministère, remettre les différentes cartes d'identité et d'accès, les actifs informationnels ainsi que tout l'équipement informatique ou de téléphonie mise à sa disposition dans le cadre de ses fonctions.

8. DROIT DE REGARD

Le sous-ministre a droit de regard sur l'utilisation des actifs informationnels par les employés. Ainsi, il peut avoir accès à toute information consignée sur l'équipement électronique du ministère, au moyen du courriel, d'un collecticiel ou des services d'Internet ou par tout autre moyen.

Lorsque les circonstances le justifient, le sous-ministre peut appliquer des mesures de gestion sur les actifs informationnels du ministère, notamment en soumettant une personne visée à une vérification particulière de l'utilisation qu'elle fait de ceux-ci ou de l'information contenue dans les fichiers personnels de cette dernière.

Le sous-ministre doit effectuer des vérifications régulières de l'utilisation de ses actifs informationnels pour des motifs opérationnels et procéder à l'analyse de leurs résultats.
Ce droit de regard sera exercé conformément à la loi, notamment à l'égard de la protection de la vie privée, des renseignements personnels et des autres renseignements de nature confidentielle.

9. SANCTION

Le sous-ministre détermine, selon la nature ou la gravité du cas, s'il est opportun d'appliquer des mesures administratives ou disciplinaires lorsqu'une personne visée contrevient à cette politique ou à la loi.

Le sous-ministre peut aussi transmettre à toute autorité judiciaire les informations colligées qui le portent à croire qu'une infraction à toute loi ou à tout règlement en vigueur a été commise.

10. MODALITÉS DE RÉVISION

La politique doit être révisée par les autorités du ministère de la Sécurité publique conjointement avec les membres du comité ministériel de sécurité, annuellement ou lors de changements majeurs (par exemple : organisationnel, environnement technique modifié, nouvelles conditions légales, stratégies d'affaires différentes, etc.).

La responsabilité de cette révision incombe au responsable ministériel de la sécurité de l'information numérique. Cette révision s'assure que le contenu du document est toujours en adéquation avec les exigences du ministère de la Sécurité publique en matière de sécurité de l'information. Une révision efficace de la politique de sécurité consiste à :

- Vérifier que les directives et procédures décrites sont effectivement appliquées;
- Faire le point sur les événements de sécurité qui ont eu lieu auparavant (analyse des audits, traces des événements et des incidents : mesures correctives s'il y a lieu);
- Vérifier que les changements qui ont eu lieu au sein du ministère, qu'ils soient techniques ou organisationnels, ne nécessitent pas d'adaptation des politiques : actions préventives;
- Organiser la mise en place des modifications qui apparaissent comme nécessaires;
- Communiquer les résultats de la révision aux employés;
- Diffuser la nouvelle politique.

-

11. DISPOSITIONS FINALES

Le responsable organisationnel de la sécurité de l'information est chargé de la mise en œuvre des dispositions de la présente politique et de ses directives d'application.

La présente politique est complétée par le cadre de gestion de la sécurité de l'information. Les obligations qui en découlent sont précisées par des directives.

La présente politique entre en vigueur à la date de sa signature par le sous-ministre.

_____ _____

Sous-ministre Date

ANNEXE A : DÉCLARATION D'ENGAGEMENT PAR LES UTILISATEURS QUANT AU RESPECT DES RÈGLES DE SÉCURITÉ DE L'INFORMATION

Les utilisateurs ont l'obligation de protéger les actifs informationnels mis à leur disposition par le ministère. À cette fin, ils doivent :

- Se conformer aux directives gouvernementales, à la politique sur la sécurité de l'information ainsi qu'aux directives, aux standards, aux procédures et aux autres lignes de conduite touchant la sécurité de l'information du ministère;
- Utiliser, à l'intérieur des droits d'accès qui leur ont été conférés et uniquement lorsqu'ils sont nécessaires à l'exercice de leurs fonctions, les actifs informationnels mis à leur disposition en se limitant aux fins auxquelles ils sont destinés;
- Respecter les mesures de sécurité mises en place sur leur poste de travail et sur tout équipement contenant des données à protéger et ne pas modifier la configuration des mesures de sécurité ni les désactiver;
- Se conformer aux exigences légales portant sur l'utilisation des produits à l'égard desquels des droits de propriété intellectuelle pourraient exister;
- Signaler immédiatement à leur supérieur tout acte, dont ils ont connaissance, susceptible de constituer une violation réelle ou présumée des règles de sécurité ainsi que toute anomalie pouvant nuire à la protection des actifs informationnels du ministère;
- Au moment de leur départ du ministère, remettre les différentes cartes d'identité et d'accès, les actifs informationnels ainsi que tout l'équipement informatique ou de téléphonie qui avaient été mis à leur disposition dans le cadre de leurs fonctions.

Moi, _____, je reconnais avoir pris connaissance des règles, ci-dessus reproduites, sur la sécurité de l'information du ministère et m'engage à les respecter.

Signature : _____

Date: _____

ANNEXE B : LEXIQUE

Actif informationnel : Une information, une banque d'information, un système ou un support d'information, une documentation, une technologie de l'information, une installation ou un ensemble de ces éléments, acquis ou constitué par le ministère.

Antivirus : Logiciel de sécurité destiné à prévenir, à détecter ou à supprimer toute présence de virus dans un système informatique.

Calendrier de conservation : Instrument de gestion documentaire élaboré en vertu de la Loi sur les archives.

Code d'utilisateur : Code alphanumérique attribué par la Direction des technologies de l'information pour identifier un utilisateur et pour définir l'usage qu'il peut faire des actifs informationnels du ministère.

Collecticiel : Logiciel qui permet à des utilisateurs reliés par un réseau de travailler en collaboration sur un même projet.

Cycle de vie de l'information : L'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 de l'organisme public.

Détenteur : Personne désignée responsable par délégation du sous-ministre, aux fins de sécurité, d'une ressource informationnelle dont le ministère est propriétaire.

Document : 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 symboles, 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 à un autre. Est également assimilée au document toute banque de données dont les éléments structurants permettent la création de documents par la structuration de l'information qui y est inscrite.

Droit d'auteur : Droit exclusif de produire ou de reproduire une œuvre ou une partie importante de celle-ci, sous une forme matérielle quelconque, de la présenter en public, de la publier, de permettre l'un de ces actes ainsi que tous les droits accessoires y afférents comme il est défini par la Loi sur le droit d'auteur.

Direction des technologies de l'information : La DTI est responsable de la sécurité des logiciels et des équipements informatiques et de réseautique; elle comprend à la fois les processus, tels que la réalisation du schéma de configuration, l'inventaire et la tenue des dossiers, et les outils.

Examen administratif : Recherche objective, indépendante, méthodique et rigoureuse demandée par les autorités du ministère sur les décisions, gestes et actes d'un employé ou incident survenu dans le cadre de ses fonctions et qui apparaissent non conformes, ou sur toute situation ou événement particulier jugé d'intérêt par une direction générale ou un gestionnaire.

L'habilitation / le contrôle des accès : L'habilitation permet à un ministère ou à un organisme d'attribuer des droits d'accès, des autorisations et des privilèges à une personne ou à un objet.

L'habilitation / le contrôle des accès : L'habilitation permet à un ministère ou à un organisme d'attribuer des droits d'accès, des autorisations et des privilèges à une personne ou à un objet.

Information : Élément de connaissance concernant un phénomène et qui, pris dans un contexte déterminé, a une signification particulière.

Réseau informatique : Ensemble des composantes et des équipements informatiques reliés par voie de télécommunications pour accéder à des ressources ou à des services informatisés, ou pour partager cet accès.

Ressource informationnelle : Ressource utilisée par le ministère, 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.

La surveillance : La surveillance sert à déceler les lacunes, à proposer des pistes pour la vérification et à protéger contre les tentatives d'intrusion et les programmes malicieux.

Système d'information : Ensembles de pratiques et des moyens servant à recueillir, à traiter, à mettre à jour, à reproduire et à distribuer les types d'information nécessaire au fonctionnement du ministère ou de l'une de ses unités

ANNEXE C : CADRE LÉGAL ET ADMINISTRATIF

Le volet juridique est un des aspects à intégrer dans l'élaboration et la mise en oeuvre d'une politique de sécurité de l'information. La présente politique a donc été conçue et doit être appliquée et interprétée en fonction des lois, des règlements, des directives et des normes suivants :

- 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 l'administration publique (L.R.Q, c. A-6.01;
- Loi sur les archives (L.R.Q., c. A-21.1), en ce qui a trait aux exigences relatives à la protection et à la conservation des documents ayant une valeur patrimoniale ou archivistique;
- Loi concernant le cadre juridique des technologies de l'information (L.R.Q., c. C-1.1);
- Charte des droits et libertés de la personne du Québec (L.R.Q., c. C-12) et la Charte canadienne des droits et libertés, Annexe B de la Loi de 1982 sur le Canada, 1982, c. 11 (R-U);
- Code civil du Québec (L.Q., 1991, c.64), notamment les articles 36 et 37, qui portent respectivement sur le respect de la vie privée et la communication des renseignements confidentiels Loi sur la fonction publique (L.R.Q., c. F-3.1.1);
- Code criminel du Canada (L.R.C., 1985, c. C-46), notamment les articles 342.1, 366 et 430, qui portent respectivement sur l'interception frauduleuse d'informations, la falsification des documents et les méfaits;
- Loi sur la fonction publique (L.R.Q., c. F-3.1.1), notamment les articles 4 à 9, et plus particulièrement les dispositions du Règlement sur les normes d'éthique, de discipline et le relevé provisoire des fonctions dans la fonction publique traitant des normes d'éthiques et de disciplines dans la fonction publique québécoise;
- Règlement sur l'éthique et la déontologie des administrateurs publics, Loi sur le ministère du Conseil exécutif (L.R.Q., c. M-30, a. 3.0.1 et 3.0.2, 1997, c. 6, a. 1);
- Loi sur le droit d'auteur (L.R.C., 1985, c. C-42);
- Loi sur les marques de commerce (L.R.C., 1985, c. T-13);
- Loi sur la protection des renseignements personnels et les documents électroniques (L.C. 2000, c. 5);
- Normes en matière d'acquisition, d'utilisation et de gestion des droits d'auteur des documents détenus par le gouvernement et les ministères et organismes désignés, en vigueur depuis le 1er novembre 2000 (A.M., 2000 : Gazette officielle du Québec, 25 octobre 2000, p.6753);
- Directive sur l'utilisation éthique du courriel, d'un collecticiel et des services d'Internet par le personnel de la fonction publique (Loi sur l'administration publique - L.R.Q., c. A-6.01, a. 31), (C.T. 198872 du 1er octobre 2002);

- Recueil des pratiques recommandées en matière de sécurité de l'information (partie 1, gestion de la sécurité, Conseil du trésor, décembre 1999);
- Directive sur la sécurité de l'information gouvernementale;
- Directive en matière d'examens administratifs et d'enquêtes;
- Directive sur la destruction des documents;
- Loi sur le ministère de la Sécurité publique.

PROJET

Sécurité publique
Québec