Pratique recommandée en sécurité de l'information

PR-074

Guide d'élaboration d'une politique de sécurité de l'information

ENSEMBLE on fait avancer le Québec

Québec

Guide d’élaboration d’une politique de sécurité de l’information

Cette publication a été réalisée par
le Sous-secrétariat du dirigeant principal de l'information
et produite par la Direction des communications
du Secrétariat du Conseil du trésor.

Vous pouvez obtenir de l'information au sujet
du Conseil du trésor et de son Secrétariat
en vous adressant à la Direction des communications
ou en consultant son site Web.

Direction des communications
Secrétariat du Conseil du trésor
2e étage, secteur 800
875, Grande Allée Est
Québec (Québec) G1R 5R8

Téléphone : 418 643-1529
Sans frais : 1 866 552-5158

communication@sct.gouv.qc.ca
www.tresor.gouv.qc.ca

Dépôt légal – juillet 2016
Bibliothèque et Archives nationales du Québec

ISBN 978-2-550-71121-6 (en ligne)

Table des matières

Remerciements

Le Sous-secrétariat du dirigeant principal de l'information remercie l'équipe de réalisation et le groupe de travail interministériel pour leur participation et le travail accompli.

Équipe de réalisation

Mohamed Darabid, coordonnateur
Secrétariat du Conseil du trésor

Makram Mourad Laribi, chargé de projet
Secrétariat du Conseil du trésor

Groupe de travail interministériel

Daniel Guimont
Commission des lésions professionnelles

Dany Michaud
Commission de protection du territoire agricole du Québec

Claude Côté
Commission des transports du Québec

Javier Betancur
Contrôleur des finances

Pierre Bonhomme
Ministère de l'Éducation, du Loisir et du Sport

Marthe-Anaïs Kambou
Ministère de la Santé et des Services sociaux

Jacques Blouin
Régie de l'assurance maladie du Québec

Mario Trudel
Société de l'assurance automobile du Québec

Notes à l'intention du lecteur

Note 1 : Le terme « organisme public » désigne un ministère ou un organisme, qu'il soit budgétaire ou autre que budgétaire, ainsi que tout organisme du réseau de l'éducation, du réseau de l'enseignement supérieur ou du réseau de la santé et des services sociaux. [Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement].

Note 2 : Le qualificatif « sectoriel » est utilisé pour désigner ce qui se rapporte à un organisme public.

Note 3 : Le qualificatif « gouvernemental » est utilisé pour désigner ce qui se rapporte à l'ensemble des organismes publics.

Note 4 : Certains termes ou acronymes sont définis dès leur première apparition dans le texte. Ces définitions sont également présentées à l'annexe I – Définitions.

Note 5 : Bien que les éléments du présent guide soient applicables à la plupart des organismes publics, il convient pour chaque organisme public de les adapter à son contexte et aux risques qui lui sont propres.

Note 6 : Le présent guide a été élaboré en prenant appui sur les normes[1] internationales de sécurité de l'information, particulièrement la norme ISO/IEC 27001 (Techniques de sécurité - Systèmes de gestion de la sécurité de l'information) et la norme ISO/IEC 27002 (Recueil de bonnes pratiques en sécurité de l'information).

1. 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.

1. Introduction

Le guide d'élaboration d'une politique de sécurité de l'information a été élaboré pour servir de référence aux organismes publics dans la définition des valeurs organisationnelles et des orientations internes en matière de sécurité de l'information, permettant ainsi d'affirmer l'engagement de la haute direction de s'acquitter de ses obligations à l'égard de la sécurité de l'information.

Il vise à soutenir les organismes publics dans l'élaboration et la mise en œuvre de leur politique de sécurité de l'information, affirmant ainsi leur engagement à soutenir les actions qui en découlent et à mettre de l'avant les moyens nécessaires à leur réalisation.

1.1 Mise en contexte

Le présent guide s'inscrit dans une démarche visant à mettre en œuvre une gouvernance forte et intégrée de la sécurité de l'information gouvernementale. Celle-ci est appuyée par :

- ✓ la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement;
- ✓ la Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics;
- ✓ quatre documents définissant le cadre de gouvernance de la sécurité de l'information dans l'administration québécoise[2];
- ✓ la politique de sécurité de l'information de l'organisme public concerné.

De plus, ce guide répond à l'obligation du dirigeant principal de l'information (DPI) d'accompagner les organismes publics et de leur apporter le soutien nécessaire dans la prise en charge des exigences de sécurité de l'information gouvernementale, notamment par l'élaboration et la diffusion de guides, pratiques et outils en la matière.

1.2 Portée et champ d'application

Le guide s'applique à l'information gouvernementale consignée dans un document[3], tel que ce terme est décrit à l'article 3 de la Loi concernant le cadre juridique des technologies de l'information (chapitre C-1.1). L'information visée est celle qu'un organisme public détient dans l'exercice de ses fonctions, que sa conservation soit assurée par lui-même ou par un tiers.

2. Les quatre documents dont il est question ici sont la Directive sur la sécurité de l'information gouvernementale, le Cadre gouvernemental de gestion de la sécurité de l'information, le Cadre de gestion des risques et des incidents à portée gouvernementale et l'Approche stratégique gouvernementale 2014-2017 en sécurité de l'information.
3. Document : Un ensemble constitué d'information portée par un support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et 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 transcrits 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 : la Loi concernant le cadre juridique des technologies de l'information – article 3

Le présent document est à l'usage des organismes publics visés par l'article 2 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (voir l'annexe II).

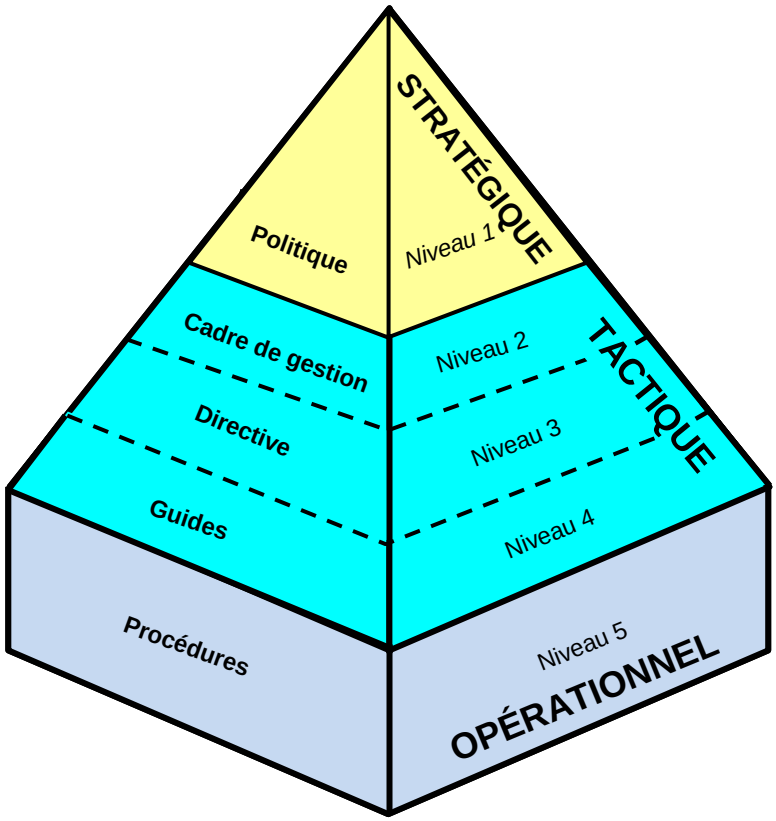
2. Rappel du cadre normatif sectoriel de sécurité de l'information

Le schéma présenté ci-dessous illustre la hiérarchie des principales composantes du cadre normatif sectoriel de sécurité de l'information. Ces composantes se traduisent notamment :

- ✓ au niveau stratégique, par la politique de sécurité de l'information;
- ✓ au niveau tactique, par le cadre de gestion, les directives et les guides;
- ✓ au niveau opérationnel, par des procédures décrivant les étapes d'un processus d'implantation ou de mise en œuvre d'une mesure de sécurité[4].

4 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

Figure 1 : Structure du cadre normatif sectoriel



2.1 Niveau 1 : Politique de sécurité de l'information

La politique de sécurité de l'information témoigne de l'importance accordée par l'organisation à la protection de l'information gouvernementale. Elle énonce des principes généraux et fixe des responsabilités à l'endroit de certains intervenants clés, notamment à l'égard des utilisateurs[5], du sous-ministre ou dirigeant d'organisme, du responsable organisationnel de la sécurité de l'information (ROSI), des gestionnaires et des détenteurs.

Par ailleurs, la politique fait référence à d'autres intervenants et aux instances internes de coordination et de concertation, dont les rôles et responsabilités sont décrits sommairement dans un document complémentaire à la politique, soit le cadre de gestion de la sécurité de l'information. Citons, à cet égard, les personnes responsables de la continuité des services[6], de la sécurité physique, de la vérification interne ou de la gestion documentaire ainsi que les

5 Utilisateur : Toute personne de l'organisation de quelque catégorie d'emploi, de statut d'employé ainsi que toute personne qui, par engagement contractuel ou autrement, utilise un actif informationnel de l'organisation ou y a accès.

6 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.

comités chargés de la sécurité de l'information ou de la protection des renseignements personnels.

Cette façon de procéder se justifie, eu égard à l'importance :

- ✓ d'adopter une politique relativement concise, facile à lire et à comprendre pour l'ensemble des utilisateurs;
- ✓ d'adopter une politique au contenu moins variable comparativement au cadre de gestion.

2.2 Niveau 2 : Cadre de gestion de la sécurité de l'information

Le cadre de gestion de la sécurité de l'information vise à compléter les dispositions de la politique. À cet effet, il précise l'organisation fonctionnelle en matière de sécurité de l'information et décrit les responsabilités de divers intervenants ainsi que les rôles des comités sectoriels.

2.3 Niveau 3 : Directives

D'application obligatoire, une directive vise à préciser, pour un domaine d'application particulier de sécurité de l'information (sécurité des locaux et des équipements, échange sécuritaire de l'information, etc.), les dispositions à respecter aux fins d'assurer la sécurité de l'information. Mentionnons, à titre d'exemple, les directives portant sur la gestion des accès à l'information, les règles à adopter par les utilisateurs des assistants numériques personnels ou la protection des supports amovibles (mémoires Flash, disques durs, etc.).

2.4 Niveau 4 : Guides

Les guides visent à faciliter l'application des prescriptions d'une politique, d'une directive ou éventuellement d'une norme, sans en avoir le caractère contraignant[7].

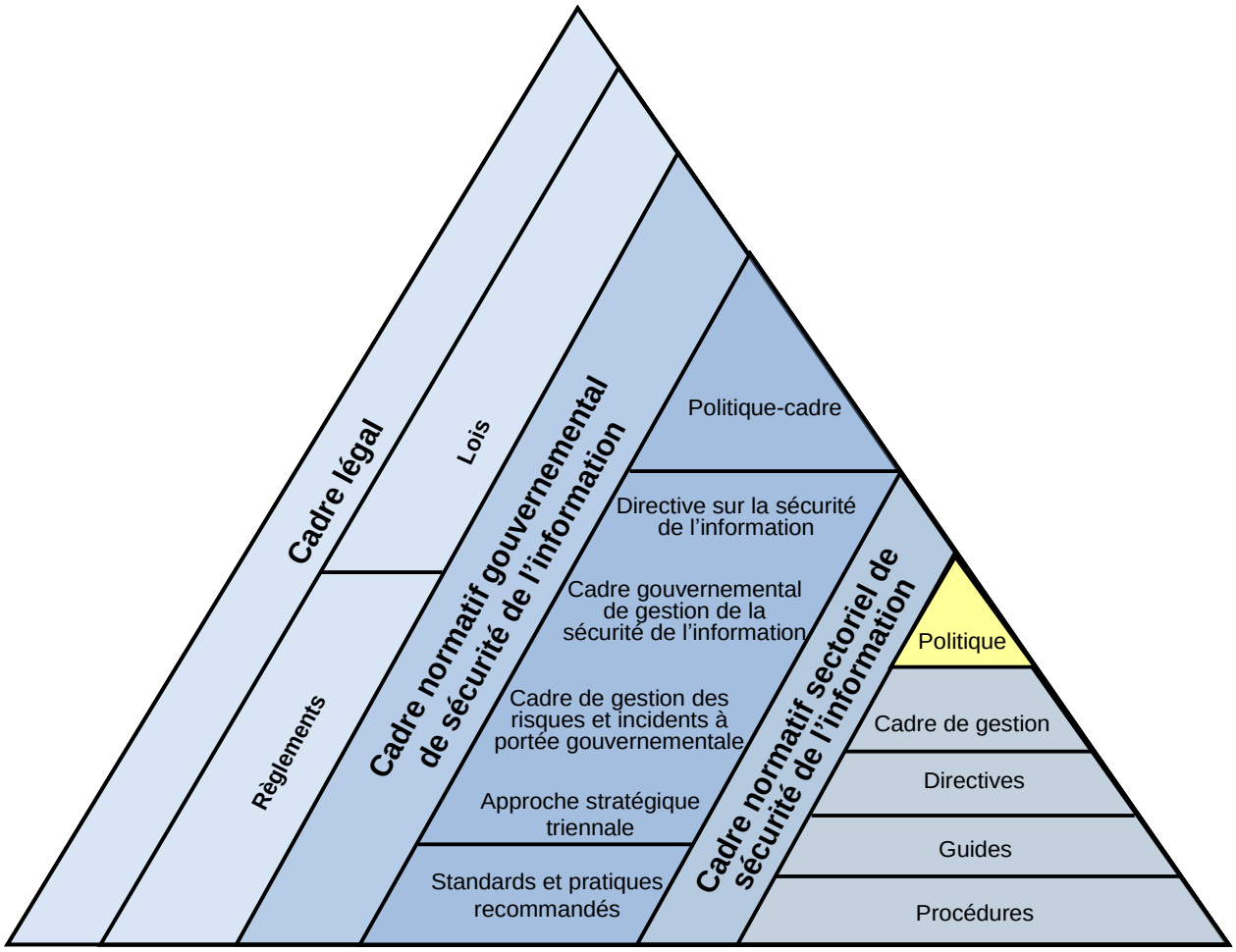
2.5 Niveau 5 : Procédures

Une procédure est un ensemble d'étapes à franchir, de moyens à prendre et de méthodes à suivre dans l'exécution d'une tâche. Elle décrit en détail les étapes d'un processus humain ou technologique d'implantation ou d'application d'une mesure de sécurité, qu'elle soit administrative ou technologique. Citons, à titre d'exemple, les procédures se rapportant à la délivrance ou la révocation des cartes d'accès, à la destruction sécuritaire des documents administratifs ou à l'attribution des mots de passe.

7 Source : OQLF – Grand dictionnaire terminologique

3. Positionnement de la politique de sécurité

Figure 2 : Positionnement de la politique par rapport au cadre légal et normatif



Comme l'illustre la figure 2, la politique de sécurité de l'information constitue l'élément principal du cadre normatif sectoriel. Celui-ci s'appuie sur le cadre légal et sur le cadre normatif gouvernemental constitué :

- ✓ de la Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics;
- ✓ de la Directive sur la sécurité de l'information gouvernementale, du cadre gouvernemental de gestion de la sécurité de l'information, du cadre de gestion des risques et des incidents à portée gouvernementale et de l'approche stratégique triennale;
- ✓ de standards, à l'instar de ceux portant sur l'interopérabilité ou l'utilisation intégrale du français dans les technologies de l'information et des communications;

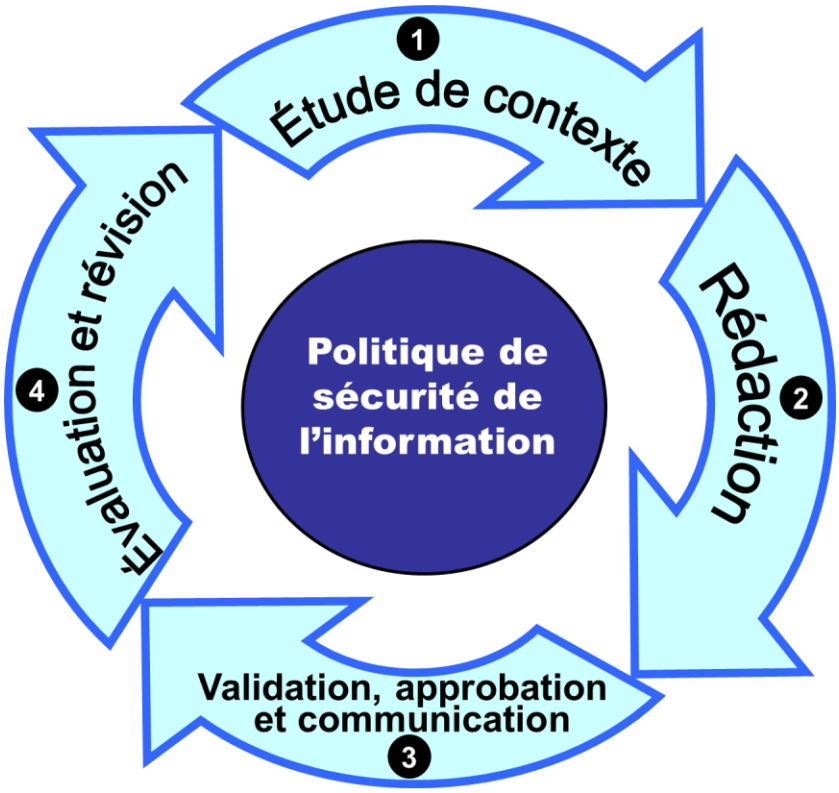
- ✓ des pratiques gouvernementales comme celles portant sur la catégorisation de l'information, l'utilisation sécuritaire des assistants numériques personnels ou la gestion des incidents.

Quant au cadre légal, il est constitué de lois, générales ou propres à un organisme public, et de règlements dont les dispositions touchent spécialement la sécurité de l'information et la protection des renseignements personnels.

4. Démarche de réalisation et de mise en œuvre

La figure présentée ci-dessous illustre la démarche préconisée pour la réalisation d'une politique de sécurité de l'information. Elle s'inscrit dans une logique d'amélioration continue et se base sur l'expertise gouvernementale dans la rédaction de pratiques exemplaires.

Figure 3 : Étapes de réalisation d'une politique de sécurité



4.1 Étude de contexte

La détermination des composantes d'une politique de sécurité de l'information prend appui sur :

- ✓ le cadre légal et le cadre réglementaire, gouvernemental et sectoriel, décrits à la section 0;
- ✓ les normes et standards de l'industrie;

- ✓ la mission de l'organisation et les risques auxquels elle est exposée;
- ✓ les priorités d'actions gouvernementales;
- ✓ tout autre document pertinent tel que les orientations gouvernementales, les recommandations du vérificateur général, les recommandations du vérificateur interne, etc.).

4.2 Rédaction

Pour l'élaboration de leur politique de sécurité de l'information, les organismes publics pourront s'appuyer sur le modèle « Politique de sécurité de l'information - modèle générique ».

Les principaux éléments à considérer dans le cadre de cette étape sont :

- ✓ le contexte d'adoption, lequel mettra l'accent sur la nécessité de renforcer le cadre de gouvernance de la sécurité de l'information de l'organisation, en établissant les conditions générales visant à préserver adéquatement la confidentialité, à garantir l'intégrité et à assurer la disponibilité de l'information;
- ✓ la terminologie et les acronymes utilisés;
- ✓ les lois, les règlements, les directives, les normes et les standards applicables sur lesquels la politique prendra appui;
- ✓ l'objectif visé, notamment l'engagement officiel de la haute direction à soutenir la prise en charge des exigences de sécurité de l'information et à mettre de l'avant les moyens nécessaires à leur réalisation;
- ✓ le champ d'application de la politique, notamment toute personne, physique ou morale, ayant accès, sur place ou à l'extérieur des locaux de l'organisation, aux actifs informationnels desquels un organisme public a la responsabilité d'assurer la sécurité;
- ✓ les énoncés de principes généraux, notamment l'adhésion d'un organisme public aux objectifs stratégiques gouvernementaux et son engagement à ce que les solutions retenues correspondent aux pratiques exemplaires en matière de sécurité de l'information, tant sur le plan national que sur le plan international;
- ✓ les obligations des acteurs clés en matière de sécurité de l'information, comme le dirigeant d'organisme ou le ROSI, et celles des utilisateurs des actifs informationnels de l'organisation, qu'il s'agisse d'un gestionnaire, d'un employé, d'un partenaire d'affaires, d'un fournisseur ou d'un mandataire agissant pour le compte d'un organisme public;
- ✓ les sanctions auxquelles s'expose tout utilisateur contrevenant aux dispositions de la politique ou à ses directives d'application. De telles sanctions devront être conformes aux dispositions des conventions collectives, des ententes et des contrats. Elles peuvent inclure la suspension de privilège, la réprimande, etc.;
- ✓ les dispositions finales, notamment son approbation par le dirigeant de l'organisme public et sa mise en œuvre par le ROSI, sa date d'entrée en vigueur et ses modalités de révision.

4.3 Validation, approbation et communication

La validation de la politique de sécurité nécessite la contribution des entités administratives de l'organisation et du comité chargé de la sécurité de l'information. La politique de sécurité est approuvée par le sous-ministre ou le dirigeant d'organisme.

Une fois approuvée, la politique est diffusée, auprès de l'ensemble du personnel de l'organisation, en utilisant les moyens appropriés dont :

- ✓ les sites Web (intranet ou extranet);
- ✓ les trousses de sensibilisation à la sécurité de l'information;
- ✓ les bannières publicitaires sur le site intranet ou extranet;
- ✓ les articles dans les journaux internes;
- ✓ etc.

Il convient également d'organiser, à l'intention de l'ensemble du personnel, des séances de formation et de sensibilisation, afin de s'assurer d'une bonne compréhension des énoncés de la politique.

4.4 Évaluation et révision

La politique de sécurité est régulièrement évaluée, notamment en ce qui a trait à la pertinence de ses énoncés à l'égard des nouveaux enjeux de sécurité de l'information.

Une fois l'étape d'évaluation terminée, la politique pourra faire l'objet d'une révision qui assurera l'adéquation de ses énoncés aux besoins de l'organisation en matière de sécurité de l'information.

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 d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées et de n'être divulguée qu'à celles-ci.

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.

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

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

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.

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

Ressources informationnelles : Les actifs informationnels ainsi que les ressources humaines, matérielles et financières directement affectées à la gestion, à l'acquisition, au développement, à l'entretien, à l'exploitation, à l'accès, à l'utilisation, à la protection, à la conservation et à l'aliénation de ces actifs.

Standard : Norme qui n'a été ni 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.

Utilisateur : Toute personne de l'organisation de quelque catégorie d'emploi, de statut d'employé ainsi que toute personne qui, par engagement contractuel ou autrement, utilise un actif informationnel de l'organisation ou y a accès.

ANNEXE II Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement - article 2

LRQ, chapitre G-1.03

LOI SUR LA GOUVERNANCE ET LA GESTION DES RESSOURCES INFORMATIONNELLES DES ORGANISMES PUBLICS ET DES ENTREPRISES DU GOUVERNEMENT

CHAPITRE I
Article 2. Pour l'application de la présente loi, sont des organismes publics :

1° les ministères du gouvernement;

2° les organismes budgétaires énumérés à l'annexe 1 de la Loi sur l'administration financière (chapitre A-6.001), à l'exception de ceux mentionnés au paragraphe 5°, et la Sûreté du Québec;

3° les organismes autres que budgétaires énumérés à l'annexe 2 de cette loi, à l'exception de ceux mentionnés au paragraphe 5° et de l'Agence du revenu du Québec, de même que la Commission administrative des régimes de retraite et d'assurances, la Commission de la santé et de la sécurité du travail, le Conseil de gestion de l'assurance parentale dans l'exercice de ses fonctions fiduciaires, la Régie des rentes du Québec et la Société de l'assurance automobile du Québec dans l'exercice de ses fonctions fiduciaires;

4° les commissions scolaires, le Comité de gestion de la taxe scolaire de l'île de Montréal, les collèges d'enseignement général et professionnel et les établissements universitaires mentionnés aux paragraphes 1° à 11° de l'article 1 de la Loi sur les établissements d'enseignement de niveau universitaire (chapitre E-14.1);

5° les agences de la santé et des services sociaux et les établissements publics visés par la Loi sur les services de santé et les services sociaux (chapitre S-4.2), les personnes morales et les groupes d'approvisionnement en commun visés à l'article 383 de cette loi, le Conseil cri de la santé et des services sociaux de la Baie James institué en vertu de la Loi sur les services de santé et les services sociaux pour les autochtones cris (chapitre S-5), les centres de communication santé visés par la Loi sur les services préhospitaliers d'urgence (chapitre S-6.2), le Commissaire à la santé et au bien-être, la Corporation d'urgences-santé, Héma-Québec, l'Institut national d'excellence en santé et en services sociaux, l'Institut national de santé publique du Québec et l'Office des personnes handicapées du Québec;

6° les autres organismes désignés par le gouvernement.

Sont considérées comme des organismes budgétaires ou autres que budgétaires les personnes désignées ou nommées par le gouvernement ou par un ministre, avec le personnel qu'elles dirigent, dans le cadre des fonctions qui leur sont attribuées par la loi, le gouvernement ou le ministre et qui sont respectivement énumérées aux annexes 1 et 2 de la Loi sur l'administration financière.

2011, c. 19, a 2.

ANNEXE III Politique de sécurité de l'information - modèle générique

N. B. Le présent modèle a été rédigé pour s'appliquer à un ministère. Il peut être adapté pour s'appliquer à tout organisme public.

TABLE DES MATIÈRES

1. Préambule

La présente politique a été 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. Définitions

Actif informationnel : Tout document dont la définition correspond à celle de l'article 3 de la Loi concernant le cadre juridique des technologies de l'information (chapitre C-1.1). À titre de rappel, cette loi définit le document comme étant : « Un ensemble constitué d'information portée par un support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcrit sous l'une de ses formes ou en un autre système de symboles ».

Cette même loi assimile 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.

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

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.

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

Intégrité : Propriété associée à une information de ne subir aucune altération ou destruction sans autorisation et d'être conservée sur un support lui procurant stabilité et pérennité.

3. Cadre légal et administratif

La politique de sécurité s'inscrit principalement dans un contexte régi par :

- ✓ la Loi sur le ministère[8];
- ✓ la Charte des droits et libertés de la personne (LRQ, chapitre C-12);
- ✓ le Code civil du Québec (LQ, 1991, chapitre 64);

8 Fait référence à la loi constitutive du ministère auquel la présente politique s'applique.

- ✓ la Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics;
- ✓ la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LRQ, chapitre G-1.03);
- ✓ la Loi concernant le cadre juridique des technologies et l'information (LRQ, chapitre C-1.1);
- ✓ la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (LRQ, chapitre A-2.1);
- ✓ la Loi sur les archives (LRQ, chapitre A-21.1);
- ✓ la Loi sur l'administration publique (LRQ, chapitre A-6.01);
- ✓ la Loi sur la fonction publique (LRQ, chapitre F-3.1.1);
- ✓ la Loi canadienne sur les droits de la personne (LRC, 1985, chapitre H-6);
- ✓ le Code criminel (LRC, 1985, chapitre C-46);
- ✓ la Loi sur le droit d'auteur (LRC, 1985, chapitre C-42);
- ✓ le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (chapitre A-2.1, r. 02);
- ✓ la Directive sur la sécurité de l'information gouvernementale;
- ✓ la Directive sur les services de certification offerts par le gouvernement du Québec pendant la phase intérimaire.

4. Objectif de la politique

La présente 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, quels que soient 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.

5. 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.

6. Énoncés de principes généraux

6.1 Protection de l'information

a) 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 reconnues et généralement utilisées, tant à l'échelle nationale qu'à l'échelle internationale.

b) Le ministère reconnaît que les actifs informationnels qu'il détient sont essentiels à ses activités courantes et, de ce fait, qu'ils 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.

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

6.2 Protection des renseignements confidentiels

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

Sont notamment 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, 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.

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

6.4 Droit de regard

Le ministère exerce, en conformité avec la législation et la réglementation en vigueur, un droit de regard sur tout usage de ses actifs informationnels.

7. Obligations des intervenants clés 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 la sécurité de l'information, aux détenteurs, aux gestionnaires d'entités administratives et aux utilisateurs.

a) Le sous-ministre : il est le premier responsable de la sécurité de l'information relevant de son autorité.
b) Le responsable organisationnel de la sécurité de l'information : il assiste le sous-ministre dans la détermination des orientations stratégiques et des priorités d'intervention.
c) Le détenteur de l'information : employé désigné par le ministère, appartenant à la classe d'emploi de niveau cadre et dont le rôle est, entre autres, de s'assurer de la sécurité de l'information et des ressources qui la sous-tendent, relevant de la responsabilité de son unité administrative.
d) Les gestionnaires : ils sont chargés de la mise en œuvre des dispositions de la présente politique auprès du personnel relevant de leur autorité.
e) 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 en 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 définis dans le cadre de gestion de la sécurité de l'information, en complément à la présente politique.

8. 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 :

a) 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;
b) utiliser, dans le cadre 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;
c) 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 ou les désactiver;
d) se conformer aux exigences légales portant sur l'utilisation des produits à l'égard desquels des droits de propriété intellectuelle pourraient exister;
e) 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;

f) 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 mis à sa disposition dans le cadre de l'exercice de ses fonctions.

9. Sanctions

Lorsqu'un utilisateur contrevient à la présente politique ou aux directives en découlant, il s'expose à des mesures disciplinaires, administratives ou légales, en fonction de la gravité de son geste. Ces mesures peuvent inclure la suspension des privilèges, la réprimande, la suspension, le congédiement ou autre, et ce, conformément aux dispositions des conventions collectives, des ententes ou des contrats.

L'organisme public peut transmettre à toute autorité judiciaire les renseignements colligés et qui le portent à croire qu'une infraction à toute loi ou règlement en vigueur a été commise.

10. Dispositions finales

a) Le sous-ministre approuve la présente politique;
b) La présente politique entre en vigueur le……;
c) Le responsable organisationnel de la sécurité de l'information s'assure de la mise en œuvre des dispositions de la présente politique et de ses directives d'application;
d) La présente politique doit être révisée à l'occasion de changements qui pourraient l'affecter;
e) La présente politique sert de complément au cadre de gestion de la sécurité de l'information. Les obligations qui en découlent sont précisées dans des directives.

_____ _____

Sous-ministre Date

.

ANNEXE I ANNEXE 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 sectorielles, aux procédures et aux autres lignes de conduite se rapportant la sécurité de l'information du ministère;
- ✓ utiliser, dans le cadre des droits d'accès qui leur sont attribués 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 ou 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 l'exercice de leurs fonctions.

Je soussigné(e), _____, 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 : _____

Secrétariat
du Conseil du trésor
Québec

Au cœur de l'administration publique